AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE

HEARING

BEFORE THE

SUBCOMMITTEE ON
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 18, 2005

Printed for the use of the Committee on Financial Services

Serial No. 109–31

U.S. GOVERNMENT PRINTING OFFICE

25–573 PDF WASHINGTON : 2006

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

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. VELÁZQUEZ, 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*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

SPENCER BACHUS, Alabama, *Chairman*

WALTER B. JONES, JR., North Carolina, *Vice Chairman*
RICHARD H. BAKER, Louisiana
MICHAEL N. CASTLE, Delaware
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SUE W. KELLY, New York
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LATOURETTE, Ohio
JUDY BIGGERT, Illinois
VITO FOSSELLA, New York
GARY G. MILLER, California
PATRICK J. TIBERI, Ohio
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
RICK RENZI, Arizona
STEVAN PEARCE, New Mexico
RANDY NEUGEBAUER, Texas
TOM PRICE, Georgia
PATRICK T. MCHENRY, North Carolina
MICHAEL G. OXLEY, Ohio

BERNARD SANDERS, Vermont
CAROLYN B. MALONEY, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
LUIS V. GUTIERREZ, Illinois
DENNIS MOORE, Kansas
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
JOSEPH CROWLEY, New York
STEVE ISRAEL, New York
CAROLYN MCCARTHY, New York
JOE BACA, California
AL GREEN, Texas
GWEN MOORE, Wisconsin
WM. LACY CLAY, Missouri
JIM MATHESON, Utah
BARNEY FRANK, Massachusetts

CONTENTS

	Page
Hearing held on:	
May 18, 2005	1
Appendix:	
May 18, 2005	29

WITNESSES

WEDNESDAY, MAY 18, 2005

Fenner, Robert M., General Counsel, National Credit Union Administraton	7
Parnes, Lydia B., Director, Bureau of Consumer Protection, Federal Trade Commission	4
Thompson, Sandra, Deputy Director, Division of Supervision and Consumer Protection, Federal Deposit Insurance Corporation	5

APPENDIX

Prepared statements:	
Oxley, Hon. Michael G.	30
Bachus, Hon. Spencer	34
Hinojosa, Hon. Ruben	37
Sanders, Hon. Bernard	40
Fenner, Robert M.	44
Parnes, Lydia B.	63
Thompson, Sandra	84

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Hinojosa, Hon. Ruben:	
Letter from Consumers Union, May 17, 2005	103
Fenner, Robert M.:	
Written response to question from Hon. Sue W. Kelly	106
Parnes, Lydia B.:	
Written response to question from Hon. Sue W. Kelly	108
Thompson, Sandra:	
Written response to question from Hon. Sue W. Kelly	110
Consumers Union, prepared statement	112

ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE

Wednesday, May 18, 2005

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:04 a.m., in Room 2128, Rayburn House Office Building, Hon. Spencer Bachus [chairman of the subcommittee] Presiding.

Present: Representatives Bachus, Kelly, Hensarling, Pearce, Neugebauer, McHenry, Sanders, Maloney, Sherman, Moore, Frank, Carson, Baca, Green, Moore, Clay, and Matheson.

Chairman BACHUS. Good morning. The Subcommittee on Financial Institutions and Consumer Credit will come to order. This morning the subcommittee is continuing its hearings on data security breaches.

In the past few months there has been widely reported breaches of security at financial institutions and other stores of data about security breaches, and the subject of these hearings is whether or not there ought to be a standard notice when that occurs, what the standard of care ought to be for those who maintain consumers' personal information, and whether or not the current legislation both in Gramm-Leach-Bliley and the FACT Act and the guidance from the regulators is sufficient or whether we need to go further, whether consumers, in addition to notice, ought to have other rights or ought to be empowered further. I think the standards were just issued in March under Gramm-Leach-Bliley for the notifications, so it may be a little premature to make a final decision at this time.

We have several members that are working on legislation, I know Chairman Castle and Chairman Price are working on legislation establishing a standard. I also know Mr. LaTourette is working on legislation which would give consumers the right to freeze their credit information in the event that they felt like it was being fraudulently used as a result of a data breach.

The witnesses here today have only been given about a week to prepare for their testimony today, which is about half the time we normally like to give our witnesses, so I do apologize for that. And at this time I am going to take the opportunity to introduce our witnesses, and then I am going to yield to Mr. Sanders for an opening statement. I am going to introduce my entire opening statement for the record, but in the interest of going ahead and expe-

diting the hearing, hearing from our witnesses, I will abbreviate my opening statement.

But we have with us today the FTC Director of the Bureau of Consumer Protection, Lydia Parnes.

Ms. PARNES. Parnes.

Chairman BACHUS. Thank you.

FDIC Deputy Director of the Division of Supervision and Consumer Protection, Sandra Thompson. We welcome you, Ms. Thompson. And Ms. Parnes, am I getting it right now?

Ms. PARNES. Yes, you are.

Chairman BACHUS. Thank you. And I should have asked before the hearing. I apologize.

And NCUA General Counsel Robert Fenner. Thank you.

We look forward to hearing from the witnesses and thank them for taking time from their schedules to join us. And if you all would move the mikes up pretty close to you.

And at this time I will yield to Mr. Sanders for an opening statement.

[The prepared statement of Hon. Spencer Bachus can be found on page 34 in the appendix.]

Mr. SANDERS. Thank you very much, Mr. Chairman. And thank you very much to our panelists who are here today.

This is clearly an important issue. Identity theft and breach in security at some of our Nation's largest companies are huge issues that this committee has got to address, and I am glad that we are holding this hearing today.

According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past 5 years—that is a huge number of people—costing businesses and financial institutions some 48 billion and consumers $5 billion. Victims of identity theft pay an average of about $1,400, not including attorney fees, and spend an average of 600 hours to clear their credit reports. So we are dealing with an issue of real concern to the American people.

In addition, Mr. Chairman, since 2003, there have been a number of security breaches at some of the biggest companies in this country, threatening the financial privacy of millions of Americans. The largest one became public in February of 2003 when the FBI announced a nationwide investigation of a computer database security breach containing roughly 8 million Visa, MasterCard, and American Express credit card numbers. This breach forced many financial institutions to reissue thousands of Visa and MasterCards as a precaution against potential fraud.

But we are not just talking about credit card companies; we are talking about TimeWarner, Lowe's stores, T-Mobile USA, ChoicePoint, Lexus Nexus, Wells Fargo, Bank of America, Chevy Chase, and SunTrust. The list goes on and on.

For a variety of reasons, Social Security numbers, debit and check card information, driver's license numbers, e-mails, personal computer files, and information about student loans and mortgages are being stolen by computer hackers and other scam artists. Mr. Chairman, this has got to stop. We must make sure that identity thieves are prosecuted to the fullest extent of the law, but we must also make sure that the largest, the most profitable multinational

companies in this country do everything they can to make sure that these scam artists don't succeed in the first place.

In addition, Mr. Chairman, this committee must focus on how the outsourcing of financial service jobs to China, India, and other low-wage countries are threatening the privacy of our citizens. That is an issue I think that we can no longer ignore.

According to a study published by the consulting firm A.T. Kearney, more than 500,000 financial service jobs in the United States, representing 8 percent of all jobs in banking, brokerage, and insurance firms, will move offshore in the next 5 years, saving these companies some $30 billion. Now that is an issue unto itself from a worker perspective, but it is also a major issue in terms of the privacy issue that we are dealing with today.

It seems that no financial service firms or credit bureau agency is immune to overseas outsourcing, and we are the biggest ones doing that. One example of the troubling trend in outsourcing is occurring at TransUnion. According to David Emory, executive vice president and chief financial officer of TransUnion, quote, 100 percent of our mail regarding customer disputes is going to India at some point, end of quote.

And according to a report in the San Francisco chronicle, quote, two of the three major credit reporting agencies, each holding detailed files on about 220 million U.S. consumers, are in the process of outsourcing sensitive operations abroad, and a third may follow suit shortly, industry officials acknowledge for the first time, end of quote.

Mr. Chairman, with growing problems in identity theft and with no domestic legal protection for the privacy of the personal records of American citizens, the situation is unhappily ripe for abuse, and the evidence is mounting. It was recently reported that three former call center workers in India allegedly cheated Citibank customers in the U.S. out of hundreds of thousands of dollars. It has also been reported that Geometric Software Solutions in India, another overseas outsourcer, illegally tried to sell the U.S. clients' intellectual property. And an employee in Pakistan doing clerical work for a medical center in California threatened to post confidential medical records of U.S. patients on the Internet unless she was adequately compensated for her work.

I would like to ask that witnesses today—and I hope that this is an issue that you will cover, the following questions. Exactly what kind of legal protections do U.S. consumers have when our privacy laws are violated overseas? As I understand it, it would be difficult, if not impossible, to prosecute financial services or credit bureau workers outside of the United States for breaking laws relating to financial privacy and consumer protection. That is why I am supportive of legislation introduced by Congressman Markey that would make it illegal for companies in the U.S. to send financial data abroad without the express written consent of their customers.

Mr. Chairman, thank you again for holding this very important hearing. And I look forward to hearing our witnesses.

[The prepared statement of Hon. Bernard Sanders can be found on page 40 in the appendix.]

Chairman BACHUS. I thank the ranking member.

Are there other members that wish to make an opening statement? If not, we will hear from our witnesses. Ms. Parnes.

STATEMENT OF LYDIA B. PARNES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Ms. PARNES. Thank you. Mr. Chairman and members of this subcommittee, I am Lydia Parnes, Director of the Bureau of Consumer Protection of the Federal Trade Commission.

I want to thank you for holding today's hearing on the important issue of improving the security of consumers' personal information and reducing the risks of identity theft. The FTC staff greatly appreciate the leadership of Chairman Bachus, Representative Sanders, and the Financial Services Committee in the recent revisions to the Fair Credit Reporting Act. And I look forward to working with you on this issue as well.

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

Americans are very concerned about the security of their personal information, and for good reason. All told, each year identity theft costs American businesses $48 billion and consumers $5 billion more. Not surprisingly, there is a direct correlation between the type of identity theft and its cost to victims. According to an FTC survey, although people who had new accounts opened in their names made up only one-third of the victims, they suffered two-thirds of the harm.

The Commission has worked hard to assist victims and to educate consumers and businesses about the risks of identity theft. We facilitate cooperation, information sharing, and training among Federal, State, and local law enforcement. The Commission maintains a Web site and a toll-free hotline to respond to the 15,000 to 20,000 inquiries we receive each week, and our trained counselors advise victims on how to reclaim their identities. In addition, many of the recent revisions to the Fair Credit Reporting Act are designed to assist victims of identity theft, and the Commission is working hard to implement these provisions.

The recent breaches of consumer information have focused attention on the practices of data brokers that collect and sell information for a wide variety of purposes. Despite the potential benefits of these information services, as recent events demonstrate, if the sensitive information they collect gets into the wrong hands, it can cause serious harm to consumers.

A variety of laws and regulations address the security of and access to sensitive information that these companies maintain. When breaches occur, the Commission staff takes a close look to determine if existing laws have been violated. Although such investigations are nonpublic, ChoicePoint has publicly acknowledged that it is under investigation by the FTC.

The recent breaches raise the question of whether existing laws are sufficient to protect consumers' information, and new legislation in fact could be useful. As FTC Chairman Majoras has testified, the most immediate need is to address the risks to the security of the information. At the outset, companies should take steps

to prevent breaches before they happen. Therefore, it makes sense to impose substantive security requirements on data brokers and other entities that collect sensitive personal information, much like the security requirements imposed under the Commission's safeguards rule.

Another step to consider would be a workable Federal requirement for notice to consumers when there has been a security breach that raises a significant risk of harm to consumers. As was the case in this committee's consideration of the FACT Act, the challenge is to fashion effective consumer protection while preserving the benefits that legitimate information services provide to consumers and the economy.

Mr. Chairman, members of the subcommittee, the FTC shares your concern for the security of consumer information, and we will continue to take steps within our authority to protect consumers.

Thank you for the opportunity to discuss this vitally important subject, and I am happy to respond to your questions.

Chairman BACHUS. Thank you.

[The prepared statement of Lydia B. Parnes can be found on page 63 in the appendix.]

Chairman BACHUS. Ms. Thompson.

STATEMENT OF SANDRA THOMPSON, DEPUTY DIRECTOR, DIVISION OF SUPERVISION AND CONSUMER PROTECTION, FEDERAL DEPOSIT INSURANCE CORPORATION

Ms. THOMPSON. Thank you, Chairman Bachus, Ranking Member Sanders, and members of the subcommittee. I appreciate the opportunity to testify before this subcommittee on behalf of the FDIC. I cannot overemphasize the importance we place on data security and protecting sensitive information. As well as causing financial harm and emotional distress to consumers, the failure or misuse of data security can impact the safety and soundness of an institution and undermine confidence in the banking system and the economy.

My oral statement this morning will briefly describe some of the emerging trends and developing threats we see in terms of security breaches. I will also discuss the FDIC's examination programs, and I will touch on our outreach efforts to the industry and consumers.

The Internet has made it possible to build a virtual storefront that criminals can use to conduct business.

Malicious software on users' computers, phishing, schemes, and pharming technologies are all aimed at consumers. Financial institutions and companies that store, transport, and use consumers' information are also targets.

Phishing continues to increase and now comprises over 50 percent of the incidents reported to the FDIC. Phishers have begun attacking smaller institutions, expanding their operations as the larger often phished banks become less fertile.

The FDIC recently published a study discussed in my written statement that recommends financial institutions and service providers consider stronger risk-based authentication strategies to reduce fraud related to passwords and other Internet account access vehicles. The Federal banking agencies have plans to release guidance on authentication later this year. To address the specialized nature of technology-related supervision, risks, and controls in the

banking industry, the FDIC regularly and routinely evaluates all of its regulated financial institutions' information security programs through our information technology examinations, as well as enforcing privacy requirements through our compliance examination program.

The FDIC also conducts IT examinations of the major technology service providers that support financial institutions. Through a national examination program, onsite reviews of large technology service providers are conducted on an interagency basis.

As you know, Congress has passed several key laws designed to protect personal information. These laws have become part of the business of banking and include the Gramm-Leach-Bliley Act, the Fair and Accurate Credit Transaction Act, and the Fair Credit Reporting Act. Institutions that fail to comply with these laws may face enforcement actions ranging from informal agreements to civil money penalties or other administrative actions.

The FDIC takes a proactive approach to enforcing data security regulations and guidance. If an institution's program for securing customer data is inadequate, the FDIC takes action regardless of whether or not there has been a compromise in data security. When data protection fails, financial institutions must adhere to the ″Response Program″ guidance issued by the FDIC and the other regulators in late March. The guidance is designed to address incidents of unauthorized access to sensitive customer information. Among many other things, customer notice should be given in a clear and conspicuous manner and should include a description of the incident, the types of information subject to unauthorized access, measures taken to protect the customers from further unauthorized access, a telephone number customers can call for information and assistance, and a reminder to customers to be vigilant in monitoring their account activity over the next 12 to 24 months.

With regard to outreach, the FDIC has taken an active role in reaching out to large numbers of people in the financial community to discuss cyber risks and controls. We have done this in several ways. As members with our fellow regulators in the Finance and Banking Information Infrastructure Committee, a body committed to promoting public-private partnership and improving coordination and communication among financial regulators, we hosted a series of symposia examining the security of the U.S. financial sector and identifying steps banks should take to protect themselves. To date, we have held 20 of these sessions around the country, and over 1,000 bank executives have attended.

In terms of consumer education, we recently launched a series of identity theft symposia, the first here in Washington in conjunction with National Consumer Protection Week. Given the standing-room-only crowd, we decided to do several more across the country. The idea is to bring together government, industry, law enforcement, and consumer interests to identify the scope of the identity theft problem and discuss proposed solutions. At our February symposium, we invited audience members and speakers to participate in a consumer education focus group and give us input on our education efforts and to help identify consumer needs in this area.

Finally, I would mention that our publication, the quarterly FDIC Consumer News, frequently includes articles on identity

theft. This publication goes to 60,000 subscribers besides being available on our Web site.

Mr. Chairman and members of the subcommittee, thank you for inviting us to speak on this very important topic. No amount of legislation or regulation can completely eliminate the threats to data security; however, we believe that our collaborative efforts with the industry, the public, and our fellow regulators have and will continue to significantly minimize threats.

We stand ready to work with the committee to provide any assistance to effectively address the elusive issues associated with data security.

Chairman BACHUS. Thank you.

[The prepared statement of Sandra Thompson can be found on page 84 in the appendix.]

Chairman BACHUS. Mr. Fenner.

STATEMENT OF ROBERT M. FENNER, GENERAL COUNSEL, NATIONAL CREDIT UNION ADMINISTRATION

Mr. FENNER. Thank you. Mr. Chairman and members of the subcommittee, thanks for the opportunity to present NCUA's views on this important subject of personal data security.

Chairman BACHUS. I don't think the mike is on.

Mr. FENNER. Off to a good start. Can you hear me now, Mr. Chairman?

Chairman BACHUS. That is great.

Mr. FENNER. All right. Mr. Chairman and members of the subcommittee, I want to thank you for the opportunity to present NCUA's views on this important subject of personal data security. And knowing that my written testimony is part of the record, I will be brief in my oral statement.

My written testimony is in three parts. The first part describes examples of data security breaches that NCUA has encountered involving credit unions and credit union members. It is our hope that this information will be useful to the committee as you continue to study this serious problem and as you consider whether additional legislative measures are appropriate.

Also, we believe these examples show that when breaches have occurred in the credit union system, NCUA and credit unions have been aggressive about taking the necessary steps both to notify credit union members and to minimize potential losses.

The second part of my testimony describes the measures that NCUA has taken to enhance data security in credit unions and to implement the provisions of the Gramm-Leach-Bliley Act and the FACT Act related to data security issues. These actions include regulations and guidelines requiring data security programs of all federally insured credit unions and regulations and guidelines which will take effect this June 1st requiring response programs in the event of security breaches. These response programs guidelines include a requirement to notify members of the credit union whenever misuse of information has occurred or is reasonably possible and to inform members of the type of information that was subject to unauthorized access or use.

Regulation and guidance to implement the relevant FACT Act provision are also well underway. Included are rules on proper dis-

posal of information—those rules took effect last December—and ongoing interagency work to develop regulations on red flag programs.

My written testimony also describes numerous other actions that NCUA has taken to keep the issue of data security in the forefront with credit unions and the interagency effort to examination and enforcement procedures. And we appreciate, by the way, the lead that both the FTC and the FDIC have taken in developing many of these rules and guidelines.

Finally, NCUA has two recommendations. First, we recommend that Congress restore NCUA's authority to examine third-party vendors that provide data processing and other services to credit unions. We note that we are the only FFIEC agency that does not possess this authority.

Also, while the vast majority of vendors are fully cooperative with NCUA, we have encountered instances of lack of cooperation, and as you can imagine, those tend to be the vendors who have something to hide. We believe that examination authority would strengthen NCUA's bargaining position in obtaining needed information quickly from vendors as well as enabling us to actually conduct full examinations in those rare cases where it becomes necessary.

Lastly, we want to note that we support Congress' consideration of whether data brokers and other nonfinancial institutions that maintain and distribute consumer data should be subject to requirements similar to those of Gramm-Leach-Bliley and the FACT Act.

Again, I want to thank you for the opportunity to appear today, and I would be happy to answer any questions.

Chairman BACHUS. Thank you.

[The prepared statement of Robert M. Fenner can be found on page 44 in the appendix.]

Chairman BACHUS. Mr. Hensarling, do you have questions?

Mr. HENSARLING. Thank you, Mr. Chairman.

Ms. Parnes, under one of the titles of Gramm-Leach-Bliley, I believe it is a criminal act to use deceptive tactics to obtain certain sensitive financial information. I understand that an ounce of prevention is worth a pound of cure, but with respect to the FTC can you give me some insight into what is going on in the enforcement side to the bad actors out there?

Mr. PARNES. Of course. Congressman, the FTC, as you know, has only civil authority; we do not have any criminal authority. On the civil side, the Commission enforces the safeguards rule which was issued under Gramm-Leach-Bliley. The rule requires financial institutions—and that would include consumer reporting agencies—or other service providers to maintain reasonable procedures to safeguard the customer information that they have. And the Commission has brought cases to enforce the safeguards rule.

We also enforce section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices. And the Commission has brought a number of cases challenging, as deceptive, promises that were made to keep consumers' information secure. Although the Commission has not exercised its unfairness authority, the Commission has stated that it believes that security

breaches can be unfair under the FTC Act. So we have engaged in enforcement both under Gramm-Leach-Bliley and under the FTC Act.

Mr. HENSARLING. I am still a little unclear on exactly where the trigger mechanism might be under the interagency guidance document on when a consumer would be notified that there has been a breach of security. Or are you concerned that if the trigger—or I guess to use a different metaphor, if the hurdle rate is too low, that consumers will be getting perhaps too many of these notices to where those that really do not pose a significant risk somehow detract from those that actually do, and the consumer ends up ignoring all of this disclosure to their detriment?

Ms. PARNES. I think that the trigger for notice is probably the most difficult issue here. And the issue that you are raising is precisely the concern. If consumers are inundated with notices, there are two potential problems: One is that they may put fraud alerts on their consumer reports when there really is no problem, and that can cause—that can create problems for consumers and for the industry as well.

On the other hand, they may get so many notices that they just start ignoring them, and when there is a notice that represents a real threat, they won't act on it. So I think that is a balance that we will have to consider.

Mr. HENSARLING. Ms. Thompson.

Ms. THOMPSON. I would like to add to that, because the banking regulators spend a considerable amount of time trying to determine the threshold. And I think that in the ″Response Guidance″ that we recently issued in March, the threshold for customer notification was after the institution conducts an investigation on the incident and there is clear evidence that misuse has occurred or there is a reasonable possibility that misuse is likely to occur, then that sets the threshold for the customer notice. But, again, we did want to strike a balance and make sure that customers and consumers were not inundated with notices that would over time become meaningless. But the agencies did spend a considerable amount of time on this issue.

Mr. HENSARLING. I was pleased to see in the interagency guidance that it seemingly avoids kind of a one-size-fits-all approach. Ms. Thompson, can you tell us why the security and notification guidelines might be different for Citibank and First State Bank of Athens, Texas, in the Fifth Congressional District of Texas?

Ms. THOMPSON. Congressman, I would be happy to. We believe that it is inappropriate to have the same procedures for small and large institutions. There are approximately 8,000 institutions that have Federal deposit insurance, and they range from the very small community banks to the large institutions. And the risk profiles for each bank are significantly different. For example, a small community bank would typically offer limited Internet banking services to retail customers and/or small businesses; whereas a large institution, such as the one that you have mentioned, would have very extensive Internet access and sophisticated online services that would entail a much greater risk to the bank and its customers. We believe that the controls that are in place should be

commensurate with the risk and that each institution poses a different risk.

Mr. HENSARLING. My time has expired. Thank you. Thank you, Mr. Chairman.

Chairman BACHUS. Thank you. Mr. Moore.

Mr. MOORE OF KANSAS. Mr. Chairman, I thank the witnesses for being here this morning. I just want to listen to the testimony and the other questions. Thank you, sir.

Chairman BACHUS. Thank you.

Mr. Neugenbauer.

Mr. NEUGENBAUER. Thank you, Mr. Chairman.

I think the first question I would have to the panel is that once these breaches have occurred and this personal data is out into somewhat of a public domain, what are some of the remedies or things that we can do or the public can do? Do they need to start changing their driver's license numbers? I mean, obviously you can't change their birthday, although some of us might would like to do that. But what are some of the things that we can do and the industry can do to help mitigate the issue once we do have a breach?

Ms. PARNES. Well, Congressman, I will respond to that, but I think that your question really underscores the fact that once there has been a breach, that horse is out of the barn. You know, it really becomes a problem for consumers. And so in the first instance we really think that data brokers need to focus on security procedures, safeguards. And, in fact, all businesses that maintain personal sensitive information should have safeguards that they apply to personal information that they maintain.

When there has been a breach, though, the FACT Act has provided a number of new protections for consumers who may be ID theft victims. For example, identity theft victims can place a fraud alert on their credit report. They can obtain from creditors the business records of the fraudulent accounts that were opened in their name. And that is a very important new right for consumers. They can get multiple free credit reports throughout the year to check to see if there are still problems being caused by the identity thief, and they can get information about the bad accounts that were opened by identity thieves. I would say victims of identity theft are also encouraged to contact the FTC either on our Web site or our toll-free number because we do have really a library of very good advice for consumers. The information that we have gives them step-by-step advice on how to regain their good name and model forms that they can use.

Mr. NEUGENBAUER. I think this second question, Ms. Thompson, how important is the data sharing that is going on today? I mean, we have data brokers and information brokers, and, you know, how—I mean, I think one of the concerns we have is it is just probably a lot of people that have a lot of information, probably no telling how many people have information about me individually. What is the impact on commerce if we just start saying to individuals and institutions and banks is we just don't share that information maybe other than with for credit reporting or—but selling lists and that type of thing. What impact would that have?

Ms. THOMPSON. Well, Congressman, data brokers don't come under the authority of the FDIC, so I will speak to what happens in financial institutions. Financial institutions are required, as you may be aware, to have opt-out provisions, and they are only allowed to share information with affiliates. The financial regulators know that financial institutions engage in activities with service providers. They outsource information. And we hold the financial institution, the bank management, and the board of directors accountable for that information whether they process it or whether it is processed by a service provider.

We conduct onsite examinations of our institutions, and in those examinations we make sure that we look at the contractual arrangements between a financial institution and a service provider because they are held to the same standards as the financial institution.

Mr. NEUGENBAUER. Ms. Parnes.

Ms. PARNES. Well, we do—data brokers do come under the Commission's jurisdiction. And I think that while consumers are very concerned about the security of their personal information, they also really care about the economic benefits that accrue to all of us based on the free flow of information in the economy. So I think that those are interests that we need to balance.

It is important for information to be secure, for personal sensitive information to be secure. It is also at the same time important for information to be able to flow so that consumers can get credit, they can get—they can, you know, purchase a car, get a mortgage with the ease that they are used to.

Mr. NEUGENBAUER. I think my time has expired, Mr. Chairman. Thank you.

Chairman BACHUS. Ms. Carson, did you? You were through, right?

Mr. NEUGENBAUER. My time has expired. I am sorry, Mr. Chairman.

Chairman BACHUS. Okay. Ms. Carson. No questions? Mr. Baca.

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

Ms. Parnes, my first question. My home State of California has been a leader in consumer notification through the 2003 laws, which require companies to notify the public about any security breach of computer data. However, according to USA Today's article in March, California is still a main target for identity theft, knowing that we have 36 million people in that area. Being the only State this year to have 1 million reported victims of identity theft, according to FTC California, Riverside, Los Angeles, San Francisco, San Diego, and my home county of San Bernardino are likely vulnerable. The article states that California's reputation as identity theft capital can be tied to major methamphetamine sales.

I am wondering if you have any comments on the link and meth labs, and how the two problems can be dealt with together.

Ms. PARNES. I am going to have to give that some thought. This is linking identity—the problem of identity theft?

Mr. BACA. With meth labs in our area, since we have quite a few in those counties, in that area, and the availability to get that. I just wanted to hear your comments. But if not, you can submit a

written statement later on and answer the question, if you don't mind.

Ms. PARNES. Thank you.

Mr. BACA. If not, my next question would be to Sandra Thompson. As you know, in your testimony, consumer data in transit, such as information stored in backup tapes and hard drives, have always been vulnerable to theft. However, the knowledge of the theft of such data can contribute to identity theft growing. Well, we know that. We know what our prison system is doing right now. What is FDIC guidance? How much sensitive information should be transported is the question number one. Does FDIC suggest that such data be encrypted to protect the information from hackers is question number two, or does the guidance encourage more common sense in physically protecting the backup tapes and hard drives?

Ms. THOMPSON. Congressman, all of the banking regulators have guidance. We have 12 examination handbooks that are available to the public, the industry, and these handbooks have the examination procedures that all of the Federal banking regulators use when they go in and conduct banking examinations on IT security systems at banks.

One of the things that is addressed in our handbooks is the transport of data. We don't recommend encryption specifically. We do suggest that data be transported in a safe and secure manner and that institutions consider using bonded services or secure vehicles to transport information.

Generally speaking, banks back up their data so that they can have a system, or the information, to return to should something take place, and this is part of the bank's business continuity plan. We don't recommend specific instructions on exactly what to do, but we do have some suggestions on how to transport data, and confidential data specifically.

Mr. BACA. Have any studies been done in reference to what I have been seeing on ″60 Minutes″ this last week on prisons and their availability to gather data and run their companies like Fortune 500 companies? Has a study been done based on the availability of our prisoners being able to obtain identity theft and the utilization of information?

Ms. THOMPSON. Congressman, I am not aware of any studies that the FDIC has conducted in that area, but I would be happy to—

Mr. BACA. I think we have got to look at it since these guys are so sophisticated right now and there is so much identity theft going on. Is there some kind of linkage that is done within our prison systems that is done outside that may affect the consumer? It is just some studies that need to be done. Hopefully, we can look at that.

My next question, since I still have got some time, is for Mr. Fenner.

As you know, FACTA requires—when reporting data to consumer reporting agencies, credit unions must use reasonable procedures to stop reporting data that has been already stolen upon notice there has been identify theft.

In your written testimony, you explain that large credit unions may be able to report identity theft almost immediately, while smaller credit unions can take even a week to report.

How would you describe reasonable procedures—and I state, reasonable procedures—and how do these procedures differ depending on the size of the credit union? Which is question number one.

And does NCUA make the recommendations to member credit unions of varying size and capabilities on how to handle the differences and notification process when there has been identity theft?

Mr. FENNER. Well, I do think that especially in the case of credit unions, where many of the institutions are very small, often run by volunteer employees, that it is important for us to distinguish and to clarify that the procedures need to be reasonable and may vary from one size institution to the next.

Now I think that in the case of very small credit unions, a reasonable procedure might be as simple as keeping paper files on situations where members file fraud alerts, or other notices, that they may have been subject to identity theft so that that credit union, which is not run on an automated system—the employees and the volunteers who run the credit union can simply know that that is a member on whom they should not be re-reporting to the consumer reporting agency what might be fraudulent information. In other larger credit unions, it is going to be more of a fully automated system, but it should be equally effective.

Mr. BACA. Yes. But there is a difference in the process between the larger ones that have an automatic system. They immediately get it, while the other ones, the system may vary. And that is what we are trying to do, is have the same kind of process.

Mr. FENNER. I don't think there is any reason that it can't be immediate in the case of a smaller credit union as soon as they receive the notice from their member.

Mr. BACA. Thank you.

Thank you, Mr. Chairman.

Chairman BACHUS. Ms. Kelly.

Mrs. KELLY. Thank you, Mr. Chairman.

I want to thank all of you for your testimony, and specifically the FDIC and the NCUA. I am discouraged, however, that the FTC only referred to the practice of phishing in its footnotes. This is my BlackBerry. It was given to me after 9/11 by the Federal Government. This morning I came in, and on my BlackBerry there are two messages. The messages are in German from people I have never heard of.

I believe that phishing is the greatest threat to consumers in our financial system, and I think it is one of the most important things that we need to look at because, unlike other forms of financial crime, even an unsuccessful phishing effort undermines confidence in the institutions whose names are stolen, and the Federal Government's ability to protect us is clearly not total.

I have on this very recently had messages coming that looked like they are coming from banks, the Bank of America, Citibank. I don't have accounts in those banks, so I immediately blank them out, but other people may open them.

I would like to read to you an article that was posted on antiphishing.org yesterday. It is called Phishing Gets Personal by John Leyden. It says, ″Fraudsters are using stolen information to lure victims into divulging additional sensitive information in a new form of phishing attack. These so-called personalized phishing attacks target individual, named account holders at specific banks. Crooks are using real information about the account holder, such as a person's name, the correct full account number, and other bank information to make the e-mails look more legitimate and, thereby, increase response rates.

″The approach contrasts with typical phishing attacks where fraudsters randomly dispatch thousands of spam e-mails without the slightest attempts to target their attacks. Personalized phishing attacks seek to supplement existing lists of stolen credentials with even more sensitive information such as ATM pin numbers or credit card CVD codes.″ And I am ending the quote there.

I think with the continued epidemic of phishing and pharming that is assaulting millions of Americans and while I know both the FDIC and the NCUA have issued guidance on this issue to their members and made information available to share with customers, I want to know when we will expect further guidance from your agencies on steps that the institutions can take to make sure that their Web sites are secure from exploitation, but also what you think we in Congress can do to stop this kind of phishing attack.

And I am going to throw that out to all three of you.

Ms. PARNES. Representative, I would be—I am happy to answer that question from the Commission's perspective.

We actually have a lot of information that we provide to consumers in terms of how to protect themselves from phishing. Our Web site provides that information as part of our consumer education.

Phishing clearly violates the FTC Act, and we have brought cases under the act challenging those practices. We have also worked with criminal authorities. And, in fact, in one of the cases that we brought, the Department of Justice acted also and the phisher was sentenced to 46 months in prison. We actually think that criminal prosecution of phishing is much more effective than civil prosecution.

I have to say, though, from our perspective, the most significant challenge in fighting this scam is not proving a law violation; it is finding the individuals who committed the violation, because they are hidden behind walls in the Internet. Often we find that they are overseas or that the transaction is crossing many borders, and it is very difficult for us to conduct those investigations and to really find those people.

One of the things that we think will help is legislation that was introduced last year, the International Consumer Protection Act, which would give the FTC additional authority to conduct investigations when the fraudsters are overseas. And while it wasn't—this was not—this was introduced last year, but not passed, we are hopeful that in this session of Congress it will be reintroduced and become law.

Mrs. KELLY. Do you think that there is a need for a Federal coordinator on consumer financial data security who could be put in a

position not only to try to track this back, but also prosecute phishing and pharming?

Ms. PARNES. I actually think that with additional tools at the Commission, if we had—if we had additional tools to go—to pursue some of these actors cross-border, I think that we would be in a good position to—in a better position to bring more enforcement actions.

But, again, I also think that there are laws in place, and I think that the criminal authorities—the Justice Department, the U.S. Attorneys—I think that if they are able to turn their attention to this, I think that they have ample authority.

Mrs. KELLY. Most of the agencies you mentioned have a lot on their plates.

Ms. PARNES. They do.

Mrs. KELLY. So I am going to ask again: Would it be a good thing for us to put together a Federal coordinator for this, to make sure that the agencies are working together to drill down on this problem? This is a growing problem. Anybody who has—it is not just on the BlackBerrys; it is on any type of electronic money transfer.

Mr. Chairman, I wonder if we could ask the FDIC if they have some specific suggestions for what we might be able to do to help you legislatively? If you would be willing to give us—to report back to this committee with a list of some specific suggestions to try to help coordination between agencies and to help you get your job done, utilizing what laws are already on the books, there may be some ways that we can integrate what is out there, because phishing and pharming—both of these, incidentally, are spelled with a PF—I don't want the farmers in my district to call me up and say, "Why are you trying to stop farming?"

But I think it is very important that we start focusing on this. And would you be willing to ask for that?

Chairman BACHUS. Sure. And we will do that. And, in fact, Ms. Kelly and I will join on a letter and outline some of the information we would like.

And I will also ask Ms. Hooley—she is working on legislation—and Chairman Pryce and Chairman Castle to join with us, along with Chairman Kelly. Chairman Kelly has actually conducted hearings for probably 2 years on this issue.

I think you were the first person on the committee to conduct those hearings.

Mrs. KELLY. Thank you.

My time is up, but I appreciate your response.

Chairman BACHUS. Thank you.

Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. And thank you, Congresswoman Kelly. I appreciate greatly what you have just discussed because those were some of my concerns. I would also add spyware into the mix of concerns.

I am also concerned about the punishment that was mentioned just a moment ago, 46 months; and that causes me some concern because, if you get 46 months, is that sufficient punishment? And I ask because a low-tech criminal can get 5 years for snatching a purse, and a high-tech criminal gets 46 months for snatching thou-

sands of purses. Is that appropriate punishment for the high-tech criminal? Are the criminal penalties sufficient?

In Harris County, the district attorney himself had his identity stolen. Is this sufficient punishment?

Would someone kindly give me a response to the query?

Ms. PARNES. Well, Congressman, as a civil enforcement agency, we would certainly have to defer to the Department of Justice with respect to the adequacy of criminal penalties. From our perspective, the fact that criminal authorities are prosecuting these frauds is an incredibly important step, and we want to see more of that.

Mr. GREEN. Would someone else care to comment? And I am pursuing it persistently because we don't want a standard that allows high-tech criminals to get slaps on the hands and low-tech criminals to get incarceration. I want all criminals to be punished appropriately.

Yes, ma'am.

Ms. THOMPSON. Congressman Green, in one case that I am aware of, it was an insider transaction, and that person got convicted for 10 years. So I am not sure that there is one particular rule or one particular sentence for every single violation.

Mr. GREEN. My next concern has to do with whether there is a market for this information. Are we finding that this is the case, that people are actually acquiring this intelligence and then they are marketing it to persons for a fee?

And if so, give me some information, if you would, please, on the extent to which this marketing takes place.

Ms. THOMPSON. Well, as you know, the Internet makes available a global market. And I think I mentioned in my opening remarks that the Internet provides a virtual store for the exchange of information.

We break identity theft into two phases: the acquiring of information, which is done through phishing or pharming, and the actual sale or misuse of that information. And we do believe and know that there is a market for that information and that that information can and will be misused and nine times out of ten ends up in cases of identity theft.

We believe at the FDIC that consumer education is really important because in phishing scams the consumer has to actively give information. And to the extent that people are aware that these types of scams are taking place, we would like to facilitate more consumer education, more consumer awareness about these issues.

Mr. GREEN. I concur with you, and I support an intelligent society, especially consumers acquiring as much intelligence as possible. But I do still have concerns about the punishments.

And I appreciate this market information because those who acquire the information, they do so with malice aforethought, and they ought to be punished severely as well. Criminals are criminals. If you are high tech, you are just a sophisticated thug, and you ought to be punished just like we punish other thugs and thieves.

Mr. Chairman, I yield back the balance of my time.

Chairman BACHUS. Thank you, Mr. Green.

Mr. McHenry.

Mr. MCHENRY. Thank you, Mr. Chairman. And thank you for having this hearing.

My question really goes to the question of whether or not we have enough regulations on the books already dealing with data security—whether or not we have enough laws on the books already for data security. And is it a question more of enforcement of the laws and regs that we have on the books, or do we need to rewrite everything?

And this really goes to the heart of the FDIC and NCUA, and so if Mr. Fenner and Ms. Thompson, if you could address this.

Ms. THOMPSON. We believe that Congress has been very proactive in the area of data security with the Gramm-Leach-Bliley Act, the Fair and Accurate Credit Transaction Act, and the Fair Credit Reporting Act, coupled with interagency guidance that provides mechanisms for financial institutions to make sure that the data is secure.

I think when Gramm-Leach-Bliley was implemented, it recommended or required that every financial institution have an information security program that goes to the institution's board of directors. And that is a very important step, coupled with the interagency guidance. Most recently, we issued ″Response Program″ guidance, in late March. We think that we have a lot of tools at our disposal to ensure that data is secure in financial institutions.

And because I think Chairman Bachus mentioned it earlier, this guidance was just issued in March, so it is a little premature for us to comment on that. But we do think that we have a lot of tools available.

Mr. FENNER. Congressman, I would agree that, for the most part, with respect to financial institutions, the laws and the regulations that we have in place and are now developing will prove adequate, including our Gramm-Leach-Bliley implementing regulations that require in our case that every credit union have a data security program and, moreover, that they have a response program to deal with instances of unauthorized access where the security program, in fact, has failed in some fashion, and also, as Ms. Thompson mentioned, the rules that we are now developing to implement the provisions of the FACT Act.

I would add that with respect to NCUA, as I mentioned in both my written and my oral testimony, there is one area where we do come up short, and that is that the other Federal financial regulatory agencies do have authority to examine third-party vendors such as data processing firms. We don't. We had that authority at one time; under a sunset provision, we have lost it. We would like to see it restored.

And it is not that we would have the intent of examining every third-party vendor that does business with credit unions, but we think just the existence of the authority provides a powerful incentive for those third parties to cooperate with us when we need information from them. And we have, in fact—since the authority sunsetted, have had instances where we haven't received full and timely cooperation. And so we think it is important to ask Congress to consider restoring that authority for us.

I would also add that I think in the case of other data brokers, nonfinancial data brokers, that it is reasonable for Congress to con-

sider whether some of the requirements that exist for financial institutions under Gramm-Leach-Bliley and the FACT Act should be imposed on other data brokers as well.

Mr. MCHENRY. So perhaps NCUA and FDIC are doing a pretty good job, and you have pretty much the tools you need aside from the tools you mentioned, Mr. Fenner. So largely, you are taking on this task already? Yes or no would be fine.

Ms. THOMPSON. Yes.

Mr. FENNER. Yes.

Mr. MCHENRY. Great. One of the best answers you can give Congress, yes or no.

A follow-up to Ms. Thompson. You mentioned interagency guidelines and the new implementation of those guidelines, and one thing that you have brought about is that the one-size-fits-all categorization for financial institutions does not work. And one of those areas is subjecting a small community bank to the same regulations you subject an international bank that has billions of dollars of assets when it comes to data security. And can you outline just a few examples of why that is the best approach?

Ms. THOMPSON. We, again, believe that it is inappropriate to require the same security procedures for small institutions that we expect for large institutions. And I think an example would be that a small community bank might just offer Internet banking services to small businesses or retail customers, and a large institution would have more sophisticated transactions. They would probably have very extensive Internet access, and the size of the transaction would be greater.

We take a look at the risk profile of each of our institutions. We conduct technology examinations based on the risk profile that is attributed to those specific institutions. And we think it is very important that the controls that are in place are commensurate with the risk.

Small institutions may have a noncomplex technology operation, or they may outsource to a service provider. And we want to make sure that our expectations are reasonable for financial institutions because we do not want to increase any burden.

Mr. MCHENRY. Thank you.

And thank you, Mr. Chairman.

Chairman BACHUS. Thank you.

Ms. Moore.

Ms. MOORE OF WISCONSIN. Well, thank you, Mr. Chairman, and thank you, panel, for this very important hearing.

Congressman McHenry really raised the questions that I had, and I appreciate his doing that. So I was prepared to pass but for the fact that I really didn't get—I don't feel that we have really gotten a full response to his question as to whether or not we think it is appropriate to have some sort of czar or something look at data security for those other industries outside of financial institutions.

I point specifically to the testimony of you, Mrs. Parnes, on pages 4 and 5, where you go through this laundry list of information the data brokers can secure. And, you know, stuff like child support payments, finding potential organ donors, locating witnesses and defendants, so on and so forth, that don't seem to come under the—

and you say in the testimony that it does not come under the jurisdiction of the Fair Credit Reporting Act. And I don't get the sense that it comes under any sort of regulatory authority that the FDIC has, and certainly none under which the NCUA is governed.

Secondly, I would—so I would like you respond to that.

I would also like to address a question to you, Ms. Thompson, relating to your insight that encrypting information—and I don't know if this is just from magnetic tapes or whether this would work for Internet services as well—that encrypting information would provide a much more secure environment for this information but for the cost.

I mean, is it just down to—is it just about the money in terms of protecting data?

And to Mr. Fenner I would just like to say, I would love to give you the authority.

Mr. FENNER. Thank you.

Ms. MOORE OF WISCONSIN. Thank you. So please respond.

Ms. PARNES. I actually haven't given any thought to whether there should be a kind of information security czar in the Federal Government. My initial response is that the agencies that have jurisdiction in this area, I think we actually work very closely together.

And so my inclination would be to say if you—

Ms. MOORE OF WISCONSIN. Excuse me. Let me interrupt because they have clocks in this institution. I am not used to that from State senate.

You specifically mentioned stuff like HIPAA, who has jurisdiction over that kind of information? Not you. You specifically said that you don't have jurisdiction over that kind of information. So I am convinced that you do a good job as it relates to the information for which you have jurisdiction. I am talking about other stuff.

Ms. PARNES. Right. So, for example, in HIPAA, HHS has jurisdiction there.

In the driver's license laws that I think we mentioned, there are States that enforce those.

And I think that what you are pointing out is really how complex this area is. There is information that is collected and used, you know, on so many different levels. Much of the information is public record information, and it is compiled by data brokers.

I am not certain, frankly, what, you know, a kind of centralized office would add to enforcement efforts here. I think that, you know, if Congress wants those of us on the Federal level to work more closely together, we certainly have with the banking regulators under the guidance of this committee—you know, give us that direction, and we will do that.

You know, I think we do. But as I have said, I am just not certain what, you know, a centralized point, what that will add.

Ms. THOMPSON. I would like to respond to your question about encryption. The agencies really tend to shy away from prescribing specific standards such as encryption because we want to have a flexible approach, and we want our institutions to use a flexible approach when they address this issue.

What works for one institution may not work for another institution. What works for the larger institutions may be cost-prohibitive

for the smaller institutions. So we try to not prescribe specific tools to accommodate certain standards. We try to establish the standard, and we try to have a flexible approach.

Encryption is something that many institutions use and many Government agencies use to protect and secure confidential data, but there are other methods to secure that data as well.

Ms. MOORE OF WISCONSIN. But it is costly. It costs. It costs a lot of money, right?

Ms. THOMPSON. It can.

Ms. MOORE OF WISCONSIN. But were it not for the cost, that would go a long way. Would you say it would go a long way in protecting information?

Ms. THOMPSON. Well, I think that any, including encryption, and that is—

Ms. MOORE OF WISCONSIN. And would the Internet as well, would that help?

Ms. THOMPSON. Well, any time you take steps to protect and secure your information, I think that goes a long way to enhancing data security. Any additional steps that people or potential criminals have to take in order to access information is helpful. We want to make sure, again, that there is a balance, there is a cost implication, and there is also an ease of use implication as well, and we want to make sure that people have the option to select the appropriate tool that fits their particular circumstance.

Chairman BACHUS. Thank you, Ms. Moore.

Mr. Pearce?

Mr. PEARCE. Thank you, Mr. Chairman. I would like to associate my comments myself with Mr. Green's comments. I have the same feeling toward the high-tech thugs. I think maybe the best punishment—locking them away in a cell maybe is not much different than some of them live already. So maybe we should lock them away and not give them access to the Internet or maybe make them write on a yellow pad and a pencil instead of giving them a computer. Maybe the best punishment might be to sentence them to use a 286 for the rest of their lives. I don't know. We need to figure out some way to redirect their creative energies.

Ms. Parnes, you noted in your testimony that the FTC holds roundtable discussions talking about steps that we can do, and if you were to characterize the outcome of your meetings the last year, what actual things have gone into practice of things that we can do, or what suggestions have you made into the system that come out of the roundtable discussions during the last year?

Ms. PARNES. Well, the last year has actually been a particularly productive one for us as we have been adopting the rules that are required under FACTA. And we have adopted already, I believe, seven or eight of the required regulations, and all of them—in working on all of those rules, we have had very productive discussions with industry, consumer groups, you know, all of the stakeholders on these issues.

If you would like, I could go through the rules that we have accomplished thus far.

Mr. PEARCE. I suspect that the thing that I would like to understand, without going through the entire list, is are we keeping up with the technology on the other side? In other words, are the proc-

esses to steal information developing faster than the process to defend against stealing of information?

Ms. PARNES. Keeping up with technology is always a difficult issue.

Mr. PEARCE. Is that a no?

Ms. PARNES. No, but—

Mr. PEARCE. Is that a no, no or—

Ms. PARNES. Well, it is hard to. And particularly when you are talking about technology in the hands of people who are engaged in fraud, you know, they try and stay a step ahead of us. We try to stay a step ahead of them.

Mr. PEARCE. Would you recommend that we make the entire concept, that is, that we have speeding violations in order that people not hit innocent bystanders, so the speeding itself becomes the criminal act?

Would you make even the prospect of sending out blanket e-mails intended to attract, even if we don't tie it down— would you make that a penalty?

Ms. PARNES. Well, you know, one of the things that we have done—

Mr. PEARCE. Would you make that a penalty, yes or no? We need to get a sense of where we can go here. The technology is developing faster than we are. We have got no tools. They are causing tremendous chaos in people's lives and financial distress in the system. What do we do?

Ms. PARNES. Well, I don't think that I would make that a crime. I think that what we are hoping happens, and we are working with industry on this, we had one of our workshops was on authentication under the Canned Spam Act, and what we are encouraging industry to develop is technology that authenticates the domain that an e-mail comes from. And I think that that would go a long way towards addressing the kind of phishing and pharming—

Mr. PEARCE. Except technology is developing faster, so that somebody is going to beat that.

Ms. Thompson, would you have a different answer? And I will ask Mr. Fenner, too. Would you have a different answer? Would you—maybe the entire process of even going out and trying to elicit information that is not going to be used in a productive fashion, would you make that illegal?

Ms. THOMPSON. Well, I think that we should work with industry, because technology is being developed to do good things as well. And to the extent that we have a misuse of technology, we need to be working with industry to make sure that we have solutions.

And I can't stress enough the collaboration that needs to take place between the Government and the private sector to address this issue because this isn't, as we heard today, just an issue for banks or financial institutions.

MR. PEARCE. Mr. Fenner, the red light is about to come on. Mr. Fenner, do you have an opinion?

Mr. FENNER. I don't have any problem with making it a crime to solicit information for purposes that are fraudulent or to further a criminal enterprise.

Mr. PEARCE. Yes, but while we are sitting here having these patient, long discussions, someone else is developing a technology this

morning that is going to get around anything that we develop. And at some point the concept of developing the technology to get around other technology in order to hurt people should be something that we concentrate on. We are going to have to make some tough, tough decisions somewhere down the road.

Thank you, Mr. Chairman.

Chairman BACHUS. Thank you.

Mr. Clay.

Wait a minute. I am sorry. Mrs. Maloney.

Mrs. MALONEY. First of all, this hearing makes it apparent that data security today is regulated by a confusing patchwork of laws and regulations that have obvious gaps and conflicts. The same personally identifiable data is subject to different protections, and its loss is subject to different remedies depending on who has it, and this doesn't make sense. So I hope that we will be moving towards a more unified approach or theory of data protection that will provide the same protection and remedies to the same sets of data no matter who has them.

And I want to note that there has been some guidance on this issue from the regulators involved, not just the banking regulators, but also NCUA has come out with some guidelines. But the FTC has not followed suit and come out with any guidelines. And I think at the least we need to encourage our regulators to come forward with consistent guidance.

So my first question is to Ms. Parnes from the FTC. Do you think guidance like that put out by the banking regulators and the NCUA is necessary for the institutions that you supervise? And if the not, why not?

Ms. PARNES. Congresswoman, we have a different relationship with industries that are subject to the FTC's jurisdiction. The FDIC is, and the bank regulators are, involved in an examination process. There is—it is a discrete industry that they are dealing with. There are a set number of members, a lot of members of the industry, but they have a very close relationship with the members of the industry. And as I said, they are—it is an examination type of relationship.

That is not what the FTC does. Our jurisdiction is extremely broad. We regulate all sectors of the economy with, you know, very specific exemptions. So, I think that the specific type of guidance that has been issued by the bank regulators would not necessarily be appropriate for the FTC.

However, the Commission issues guidance to the industries that it regulates in a different fashion. We have rules that we have adopted and implemented. Under Gramm-Leach-Bliley we have a safeguards rule, and we provide business education on how to implement that rule.

We brought a number of cases under section 5 dealing with information security, and we think that our law enforcement sets standards that industry should follow. And, again, right now, we are conducting nonpublic investigations in this area. We are learning more about this industry. And I think that it would be likely that at some point we would put out more general business guidance in this area. But, again, I think it would be a bit different from what the bank regulators do.

Mrs. MALONEY. So basically are you saying the FTC can't regulate the industry as carefully as the bank regulators?

I mean, they have their oversight. Why in the world can't the FTC have the same type of regulation? I don't get it. If you can't come out with it, then possibly we need to come forward with some legislation on it.

Ms. PARNES. Well, I think that—I certainly don't mean to suggest that the FTC can't give guidance to industries that fall within our jurisdiction. I think we can. We are primarily a law enforcement agency, and, for example—

Mrs. MALONEY. You can give guidance. And the FDIC has given guidance, and NCUA, they have all come forward trying to set more uniform guidance. Why don't you step in and give some guidance, too? This is a tremendous challenge.

Ms. PARNES. Well, you know, the issues that we are looking at right now on notice in particular, we are learning a lot about this. As we conduct these investigations, we have had many meetings with members of the industry and with consumer advocates.

The issues are complex. We are learning about them. But I would expect that we will seriously consider issuing guidance when we feel as if we have a better sense of what that should be.

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

Chairman BACHUS. Thank you.

I would say this to the panel and to the members that are still here. As far as financial institutions and credit unions are concerned, there is a standard of care in Gramm-Leach-Bliley. It is called a privacy obligation. But it is a standard of care, and it is very precise.

There are also safeguards listed, and there are three of them, and the regulators under those have a right to issue regulations, and you all are doing that. And they are pretty comprehensive as far as what those safeguards are to ensure the security and confidentiality of the customer records information, to protect against any anticipated threats or hazard to security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. So there is no lack of law when it comes to financial institutions or credit bureaus.

And the regulations are coming out. I think, as I see the problems, Mr. Fenner, you said that NCUA doesn't have the right to inspect third-party vendors, and, of course, you know CUNA and NAFCU are opposed to giving you that right so that you don't have that examination right.

So you have raised that today, and I think you raised a good issue. But I think the problem comes, and if I am hearing, your testimony is your data brokers aren't regulated by, they don't fall under this standard. They don't follow any of these safeguards. Is that right?

Ms. PARNES. Well, Chairman, data brokers could fall under the laws, and so, for example, if a data broker is a financial institution, it would fall within their, the GLB, standard.

Chairman BACHUS. Were ChoicePoint and LexisNexis—are they—were they financial institutions? Part of their operation were financial institutions. Is that correct?

Ms. PARNES. Chairman, these are—with respect to the nonpublic investigations that we have pending, these are issues that are kind of at the heart of these investigations, and they are nonpublic.

Chairman BACHUS. Okay. But I guess I will just say this, then: If part of those operations are financial institutions, they fall under Gramm-Leach-Bliley.

Ms. PARNES. That is correct.

Chairman BACHUS. If determined not to be, they would not.

Ms. PARNES. That is correct. And if they act as consumer reporting agencies, and some of them do, they would fall under—

Chairman BACHUS. A credit reporting agency.

Ms. PARNES. Exactly. The FCRA.

Chairman BACHUS. I actually am the author of the FACT Act, and it did give a lot of new rights and empowered consumers who—you know, after the fact. Now, also, by letting them see their credit reports, it protects them from actually ongoing fraud, but—and it did give them certain rights.

My question, I guess, would be under—from reading section 501 of Gramm-Leach-Bliley and the FACT Act, the regulators are already empowered, in my mind, to establish a uniform notice as a part of this, because, you know, statutorily you are asked to ensure these things and to safeguard and protect consumers. And I would think that you could come out with a uniform notice and, as far as financial institutions, you could preempt a hodgepodge of State laws where we are getting, you know, multiple notices.

Our financial institutions are having to send really 12- and 14-page notices because they have to comply with all these different States, and the end result is that the consumer doesn't know what he is getting.

But I guess I would ask you this: Do you think you have the authority presently? And if not, would you like that authority, to issue uniform notices in case of a—and, if we do, what criteria do we—we have always—this Congress, this committee, has always established as far as when a notice is required; it has gone back to the common-law definition of a significant threat or significant, as opposed to insignificant, and used that standard. Would that be the standard you would recommend? I will ask Ms. Parnes.

Ms. PARNES. Yeah. We—I think that looking at the risk of harm to consumers is absolutely an essential component of a trigger for notice.

Chairman BACHUS. And significant is the one that has been used for 300 years. Is there any reason to depart from that? If it was insignificant, you wouldn't, and you could have guidelines to what was considered significant.

Ms. PARNES. That is absolutely right. And this would be something that the Commission would certainly want to flesh out in guidelines or in rules. But, you know, again, I mean, I think, as you have indicated, you know, it is a balance on notice. And we certainly think that that is the consumer interest there.

Chairman BACHUS. And the only reason I am saying the use is significant, you have got years and years of case law as to what is significant and insignificant. And it can be—you know, there is a history there. If you came up with some new criteria or new stand-

ard, it would be—it would take literally years and court cases to establish what that meant.

Any comment on that? Ms. Thompson?

Ms. THOMPSON. Well, the FDIC has not made an official policy statement on this particular issue, but I believe that we will need specific Federal authority to preempt State laws. But with regard to the—

Chairman BACHUS. That is right, because there is no preemption in Gramm-Leach-Bliley. You are right. You are absolutely right. So when I said you could, you couldn't, because Senator Sarbanes added a provision in the Senate which did not allow for it. It didn't preempt State law. That is correct. So any legislation with a uniform standard would have to—I suppose it would have to negate the provision in Gramm-Leach-Bliley.

Ms. THOMPSON. I mentioned that in the interagency guidance in the customer notice response, there are some principles that the financial institutions have to adhere to. The notice has to be clear and conspicuous, and it also has to have a telephone number for people to call to get information.

Chairman BACHUS. In the FACT Act, we established what the notice was, and in Gramm-Leach-Bliley, the only thing we don't establish probably is when, what the trigger is.

And I guess I am asking you, is significant risk of significant harm is what has been used in other notices and other areas, and in other industries, and other statutes. I think that is the most common one. Probably 90 percent of your notices are required in that case, you know, when you are trying to minimize some damage or notice.

Ms. THOMPSON. With the interagency guidance, there is a threshold to send the notice. The threshold was again very difficult for the agencies to come up with, but it specifically states that if there has been misuse, or if there is a reasonable possibility that misuse will occur, then the notice is sent to the customers or the consumers.

Chairman BACHUS. You would have to probably go—you know, that is the reasonableness notice, but you would have to—would you distinguish between significant and insignificant?

Ms. THOMPSON. I think we have to because we want to make sure that customers and consumers are not receiving just notices that maybe over time become meaningless.

We want to make sure that when consumers receive notices that they pay attention, and that they understand the consequences of not paying attention, and that they take appropriate steps to make sure that their identities are protected. It is just a balance.

Ms. PARNES. And I would add, I think that is exactly the balance that we are looking at. And I think as we move forward on this, we will be looking at what we think is exactly the appropriate trigger for notice. I think we have to—

Chairman BACHUS. But you know the ″reasonableness″ is in almost all—you don't even need to put the word in normally because I think it is the reasonable man standard, but I think you ought to put the word in. Maybe what you do there is you say a ″reasonable anticipation of significant harm to the consumer″.

Ms. PARNES. I think that we would want to certainly on an issue—on an issue like this, if we were implementing rules on this or advising this Subcommittee, I think that we would want to give thought to the issues so that we could really identify an appropriate trigger and what appropriate language would be.

Chairman BACHUS. Thank you.

Mr. Sanders. Thank you very much. We have a vote on the floor.

Mr. SANDERS. I wanted to ask one question. I apologize for not being here for the whole hearing. I think there is an area, though, a very important area, that has not been discussed, and that is assuming that we do everything that we can to protect the American people, we all work together, there is a huge gap in this discussion, and that is what happens if a company offshores and that work is being done in India or it is being done in China? My feeling is that everything that you have told us doesn't really matter terribly much to a hill of beans.

My question would be in the event that an offshore company affiliated with a person subject to your jurisdiction violated any of the privacy provisions of GLBA, what authorities would your agency have to bring legal action against such persons? What authority would you have to bring an enforcement action against a rogue employee of such a company for violations committed in foreign countries?

Ms. THOMPSON. I would agree with you that prosecution of workers and employees overseas for data theft is difficult, but we do have existing data protection legislation and regulations in Gramm-Leach-Bliley in the implementing security guidelines. Banks have to choose their service providers carefully, and they have to make sure that they have access to the information, and they also have to continually monitor how their service providers are doing.

Mr. SANDERS. But having said that, Ms. Thompson, you would agree that—

Ms. THOMPSON. Yes. There is difficulty. Yes, I do agree with that.

Chairman BACHUS. What she is referring to is section 501.

Ms. THOMPSON. That is correct.

Ms. PARNES. And our position is that institutions that fall within our jurisdiction would be responsible for any data breaches that occur, even if they occur outside of our borders. Our kind of issue is one on enforcement and kind of tracking the violation, and there is legislation that was introduced in the last session of Congress, the International Consumer Protection Act, that was not passed, but that would be very useful in helping us with enforcement.

Mr. SANDERS. So you think we do need legislation, though?

Ms. PARNES. I think that piece of legislation would help this issue, yes.

Chairman BACHUS. Thank you.

Mr. SANDERS. Thank you very much.

Thank you, Mr. Chairman.

Chairman BACHUS. Just for the record, she is referring to the legislation introduced by Mr. Stearns in the Commerce Committee, I think, which we also have concurrent jurisdiction over. We actually—because we thought that was a good piece of legislation, we

waived our jurisdiction. But it did not—I don't think it got out of the Commerce Committee.

Mr. Markey has a different piece of legislation, which is different. I will just leave it at that.

But I, too, believe that the International Consumer Protection Act would go a long way towards solving the problem you have talked about.

We very much appreciate your testimony here today. We have votes on the floor, and I think they come at a time when this hearing would conclude. So we appreciate your testimony, and you have been very helpful. And this hearing is concluded.

Ms. PARNES. Thank you.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned.]

A P P E N D I X

July 8, 2005

Opening Statement

Chairman Michael G. Oxley

House Financial Services Committee

Enhancing Data Security: The Regulators' Perspective
May 18, 2005

We meet this morning for the second time this month to consider data security and its importance to American consumers and businesses. Our previous hearing, held in the full Committee, examined several recent high-profile security breaches that focused public attention on the vulnerabilities of companies' data security systems. Today we will hear from some of the regulators responsible for ensuring that these companies have appropriate policies and procedures in place to protect their sensitive information and safeguard their consumers from identity theft crimes.

The Federal banking regulators and Federal Trade Commission have worked hard to protect the security of sensitive information over the past several years. In late March of this year, 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 National Credit Union Administration (NCUA) published similar guidance in the *Federal Register* just a few weeks ago. These standards call for financial institutions to implement a response program to address incidents of unauthorized access to customer information and to notify affected customers as soon as possible.

This Committee has likewise devoted a great deal of time recently to enhancing data security and protecting consumers from identity theft. Last Congress, we passed strong consumer protection and anti-identity theft legislation under the leadership of my good friend from Alabama and the Chairman of this Subcommittee, Mr. Bachus.

Under the Fair and Accurate Credit Transactions Act, or FACT Act amendments to the Fair Credit Reporting Act, we established several new obligations to protect sensitive consumer information on financial institutions and other businesses. I look forward to hearing from our witnesses today about the status of the FACT Act's implementation.

Despite all the work that has been done, the recent rash of data security breaches has resulted in calls for additional legislation. More than half of the 50 states have now enacted or are considering bills that would require companies to provide notice of security breaches. Facing a looming patchwork of differing state law requirements, this Committee must consider whether a national breach notification standard would work better to protect all American consumers consistently and uniformly regardless of where they live.

Subcommittee Chairman Bachus, thank you again for holding today's hearing. I look forward to the testimony from today's witnesses and to our continued efforts on data security breach prevention.

OPENING STATEMENT OF CHAIRMAN SPENCER BACHUS
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
"ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE"
MAY 18, 2005

Good morning. The Subcommittee will come to order. This morning the subcommittee will continue its examination of data security and protecting sensitive information. Several weeks ago, the Full Committee held a hearing on this topic where we heard from representatives of companies that recently experienced data breaches. Today it is our intention to hear the regulators' perspective on this issue. I am pleased that Chairman Oxley continues to recognize the significance of this topic and has scheduled this hearing today.

Over the last several months, there have been numerous news reports describing potentially serious breaches of information security. These breaches have generally involved sensitive personal information, such as individual names plus Social Security numbers or payment card information. Although the reports of subsequent fraud associated with these breaches have been relatively low, protecting consumers after such data breaches obviously remains a primary concern. Furthermore, data breaches, even if relatively uncommon and limited in scope, undermine consumer confidence more broadly. For instance, surveys suggest the growth of on-line commerce is restrained due to fears about information security.

I do not expect companies to meet a standard of perfection. I doubt the witnesses here expect perfection either. Even the most prudent company can become the victim of a hacker or other criminal. However, it is reasonable to

expect that those who possess sensitive information will take reasonable steps to protect against the unauthorized acquisition of such information. In this regard, it is important for us to hear how the regulatory community is approaching this issue, and whether additional legislation is needed. It is also reasonable to expect that, if we decide to legislate in this area, companies should have a single uniform standard to comply with, as opposed to dozens of inconsistent standards. I see little benefit to a hodgepodge of security standards resulting from several different laws triggering consumer notices.

One of the key issues surrounding our investigation of data breaches is a question of how to inform consumers if their sensitive information is the subject of a security breach. For example, we are well aware that financial institutions must have information security programs designed to protect customer information under the Gramm-Leach-Bliley Act. The federal banking agencies also issued guidance recently with respect to the need for a bank to provide notice to its customers when information in the bank's control is the subject of a security breach. In my opinion the requirements of the law, and the guidance provided by the regulators, are appropriate. However, we need to learn more about this issue from the regulators, and that is why we are here today.

I would like to take this opportunity to welcome our witnesses. We have with us today FTC Director of the Bureau of Consumer Protection Lydia B. Parnes, FDIC Deputy Director of the Division of Supervision and Consumer Protection Sandra Thompson and NCUA General Counsel Robert Fenner. I look forward to hearing from today's witnesses and thank them for taking time from their schedules to join us.

I am now pleased to recognize the Ranking Member, Mr. Sanders, for any opening statement that he would like to make.

OPENING REMARKS OF THE HONORABLE RUBEN HINOJOSA
HOUSE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
"ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE"
MAY 18, 2005

Chairman Bachus and Ranking Member Sanders,

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.

As I noted during last week's hearing, 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.

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 were also stolen from nearly 95,000 customer checks.

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 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.

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 be arrested for crimes they did not commit. According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions $48 billion and consumers $5 billion. Victims pay an average of about $1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports.

Victims do not have to sit idly by – they can defend themselves against 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.

Furthermore, our constituents can access websites such as the BITS website created by the Financial Services Roundtable. The website helps consumers become aware of the many steps they can take to safeguard their personal information. The tips on the BITS website were adapted from the BITS white paper "Financial Identity Theft: Prevention and Consumer Assistance." The website provides guidance on how to protect your Social Security numbers and cards; your credit cards; your identity from predators on the Internet; your mail; and other topics. All of these documents are printed on the BITS website and available for download. You may access the website at www.bitsinfo.org/ci_identity_theft.html.

Having noted all of the aforementioned, the question becomes one of what, if anything, can or should Congress do to address the increasing numbers of identity theft and protect our constituents.

Yesterday, I received a letter from Consumers Union highlighting its "Have You Heard?" Column from the June 2005 *Consumer Reports,* which addresses the critical issue of identity theft. There are several recommendations in that column that I found very compelling. One of them focuses on preventing breaches from happening in the first place. It stresses how critical it is to impose strong requirements on information brokers to protect the information they hold and to screen and monitor the persons to whom they make that information available, and require creditors to take additional steps to verify the identity of an applicant when there is a sign of possible ID theft. Moreover, it recommends that Congress act to restrict the sale, sharing, posting, display, and secondary use of Social Security numbers. I ask that a copy of this letter and the column,

attached at the end of my opening remarks, be included in the official Subcommittee record.

Several bills have been introduced this Congress to address identity theft. H.R. 1078, the "Social Security Number Protection Act of 2005", introduced by Congressman Markey, caught my attention. It would direct the Federal Trade Commission to promulgate regulations to impose restrictions and conditions on the sale and purchase of social security numbers. I hope that today's witnesses will comment on this legislation, and I encourage my colleagues in the Committees on Energy and Commerce and Ways and Means, to which the legislation was referred, to hold hearings on it.

Finally, I look forward to the testimony of today's witnesses in the hope that they can provide further insight into the "Bank Data Breach Guidance" the Federal bank regulators published in the *Federal Register* on March 29, 2005; a similar guidance issued by the National Credit Union Administration; and an explanation as to why the FTC has yet to issue a similar guidance.

Having said that, Mr. Chairman, I yield back the remainder of my time.

STATEMENT BY REP. BERNARD SANDERS AT THE FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE HEARING ON PROTECTING THE FINANCIAL PRIVACY OF U.S. CITIZENS
10AM WEDNESDAY, MAY 18TH, 2005 – 2128 RHOB

Mr. Chairman, thank you for holding this important hearing. Identity theft and breaches in security at some of our nation's largest companies are huge issues that this Committee has got to deal with.

According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions $48 billion and consumers $5 billion. Victims of identity theft pay an average of about $1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports.

In addition, Mr. Chairman, since 2003, there have been a number of security breaches at some of the biggest companies in this country threatening the financial privacy of millions of Americans.

The largest one became public in February of 2003 when the FBI announced a nationwide investigation of a computer database security breach containing roughly 8 million Visa, MasterCard and American Express credit card numbers. This breach forced many financial institutions to reissue thousands of Visa and MasterCards as a precaution against potential fraud.

But, we're not just talking about credit card companies. We're talking about Time Warner, Lowe's Stores, T-Mobile USA, ChoicePoint, LexisNexis, Wells Fargo, Bank of America, Chevy Chase, and Sun Trust. The list goes on and on. For a variety of reasons social security numbers, debit and check card information, drivers' license numbers, e-mails, personal computer files, and information about student loans and mortgages are being stolen by computer hackers and other scam artists. Mr. Chairman, this has got to stop. We must make sure that identity thieves are prosecuted to the fullest extent of the law. But, we must also make sure that the largest and most profitable multi-national companies in this country do everything they can to make sure that these scam artists don't succeed in the first place.

In addition, Mr. Chairman, this Committee must focus on how the outsourcing of financial services jobs to China, India, and other cheap foreign labor markets also threatens the privacy of our citizens.

According to a study published by the consulting firm A.T. Kearney, more than 500,000 financial services jobs in the U.S., representing eight percent of all jobs in banking, brokerage, and insurance firms, will move offshore in the next five years saving these companies over $30 billion.

It seems that no financial services firm or credit bureau agency is immune to overseas outsourcing. Companies such as J.P. Morgan Chase, Citigroup, American Express, Morgan Stanley, Goldman Sachs, GE Capital, Bank of America, TransUnion, and Equifax have substantially outsourced white collar jobs.

One example of the troubling trend in outsourcing is occurring at TransUnion. According to David Emery, executive vice president and chief financial officer of TransUnion, "A hundred percent of our mail regarding customer disputes is going to go to India at some point."

And, according to a report in the *San Francisco Chronicle*, "two of the three major credit-reporting agencies, each holding detailed files on about 220 million U.S. consumers, are in the process of outsourcing sensitive operations abroad, and a third may follow suit shortly, industry officials acknowledge for the first time."

Mr. Chairman, with growing problems in identity theft, and with no domestic legal protection for the privacy of the personal records of American citizens, the situation is unhappily ripe for abuse, and the evidence is mounting.

It was recently reported that three former call center workers in India allegedly cheated CitiBank customers in the U.S. out of hundreds of thousands of dollars.

It has also been reported that Geometric Software Solutions, in India, another overseas outsourcer, illegally tried to sell a U.S. client's intellectual property.

And, an employee in Pakistan doing clerical work for a medical center in California threatened to post confidential medical records of U.S. patients on the Internet, unless she was adequately compensated for her work.

I would like to ask our witnesses hear today the following question: Exactly what legal protections do U.S. consumers have when our privacy laws are violated overseas?

Because, as I understand it, it would be difficult, if not impossible, to prosecute financial services or credit bureau workers outside of the United States for breaking laws relating to financial privacy and consumer protection.

That is why I am supportive of legislation introduced by Congressman Markey that would make it illegal for companies in the U.S. to send financial data abroad without the express written consent of their customers.

Mr. Chairman, thank you again for holding this hearing and I look forward to listening to our witnesses.

STATEMENT

OF

ROBERT M. FENNER

GENERAL COUNSEL
NATIONAL CREDIT UNION ADMINISTRATION

"ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE"

BEFORE THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

U.S. HOUSE OF REPRESENTATIVES

MAY 18, 2005

"ENHANCING DATA SECURITY: THE REGULATORS' PERSPECTIVE"

Chairman Bachus, and Members of the Subcommittee, I appreciate your invitation to present this testimony reviewing the National Credit Union Administration's (NCUA's) experiences with information systems and technology (IS&T) incidents and other security events resulting in the potential compromise of personal financial data. We also identify actions by NCUA to ensure credit unions safeguard member information and to mitigate potential losses to credit unions and members when breaches occur. We recommend that NCUA be granted examination authority over third party vendors, which would enable us to better monitor risk and protect credit union members' personal financial data.

Examples of Data Security Breaches Involving Credit Union Members

Information is provided here on types of security breaches NCUA and credit unions have experienced. These security breaches include: fraudulent email or telephone scams, known as phishing; the unauthorized storing of customer information and the ensuing theft of this information; the theft of a credit union's hard drive; and the theft of a vendor's computer. We also provide information on how NCUA and credit unions have responded to these data security incidents.

Phishing Scams

In a typical phishing scam, a false email is sent asking the recipient to click on a link to verify his or her credit union account registration. If the recipient proceeds to do so, the link directs him or her to a false website and asks for the member's credit union account number and PIN, along with other personal information. At least eight credit unions, NCUA itself, and a national credit union trade association have been affected by such fraudulent email or telephone scams to obtain personal financial information.

Later in this testimony, we describe applicable federal laws and the regulations and other guidance NCUA has issued prescribing how credit unions must respond to data security breaches, including phishing. When phishing incidents have occurred in the past, NCUA has followed and has recommended credit unions and other affected entities follow a three-prong response.

First, the affected entity should alert the regulators, the industry, and potential victims about the fraud. This notice occurs through website postings, and notices to staff, state supervisory authorities, and credit unions. These notifications are picked up by the credit union press and further disseminated to the general public. Second, the affected entity should do what it can to shut down the scam,

which, for example, could be a bogus website. This could occur by notifying the internet service provider who in turn would proceed to immediately shut down the bogus website. Third, the affected entity should gather as much information as it can and refer the scam to the appropriate law enforcement authorities, such as the FBI, the Department of Justice's Cybercrimes Unit, and the United States Secret Service.

Lawsuit versus B.J.'s Wholesale Club, Inc.

Another data security breach involving credit unions and their members is reflected in a pending civil lawsuit filed April 4, 2005 by the CUNA Mutual Group against B.J.'s Wholesale Club, Inc., in Massachusetts Superior Court. The CUNA Mutual Group is a mutual insurance company and provider of fidelity bonds and other financial services to credit unions and their members. CUNA Mutual seeks recovery for approximately $4.5 million in losses on behalf of itself and 163 credit unions who are bond policyholders.

The lawsuit alleges that B.J.'s Wholesale Club used point of sale software systems that captured and stored its customers' full magnetic strip information from their credit and debit cards after authorizing transactions. The storing of the information was in violation of the Visa and MasterCard association rules. In March 2004, a security breach committed by an unknown hacker occurred, compromising approximately 40,000 credit and debit cardholders and their related personal financial information.

The lawsuit alleges that a substantial number of credit union members had used their cards at B.J.'s and that they are now at greater risk for identity theft and for criminals to use the data to make duplicate cards to engage in fraudulent transactions. The alleged losses include fraud losses that credit unions have incurred and are unable to collect, the blocking costs for the affected cards, and expenses for reissuing affected cards.

Theft of Credit Union's Hard Drive

Another example of a breach of credit union members' data security involved a state-chartered credit union in California. During the weekend of November 15, 2003, two offices at the credit union were vandalized and a hard drive was taken. The hard drive was from the loan manager's PC. The credit union was preparing for a loan pre-approval promotion and member data had been downloaded from the mainframe computer to the PC and was being analyzed for the promotion.

Initially management believed approximately 49,000 member's names, account numbers, and social security numbers were on the hard drive. Further investigation disclosed almost 100,000 members whose data was compromised.

On Monday, November 17, 2003, the credit union contacted the local police and secret service and an investigation was begun. The credit union's investigation showed a lack of control over access to the building while remodeling was occurring over the weekend. Furthermore, the investigation revealed a lack of properly placed security cameras and a lack of controls over the credit union's electronic card keys.

The credit union sent a letter disclosing the compromise to all affected members on November 19. The credit union also hired additional staff and temporarily reorganized the call department to field the anticipated calls from members. Initially, call volume was very high but rapidly tapered off as the credit union explained what it was doing to protect the members against misuse of their personal information. To provide additional protection to members against potential fraud and identity theft, the credit union subscribed to the credit tracking system provided by the credit bureaus for one year. This allowed the credit union to review monthly reports to check for unusual activity in its members' accounts.

After the theft, the credit union reissued new electronic key cards to employees and a methodology was implemented to keep track of who had the cards and what areas they could access. The credit union moved its security cameras and added additional ones to the building's entrances. The credit union established new procedures to monitor outside contractors. The credit union revised the data processing system and installed on every PC a program that bars downloading of member data to the PC. Instead, all analysis, such as for a loan promotion, is done on a portion of the mainframe.

The cost to the credit union was substantial, not only in direct costs, but also in the amount of staff time, from the tellers to the CEO, allocated to the issue. Some months the costs exceeded 50% of net income. There are no known losses to the members relating to the theft.

Theft of Vendor's Computer

The following is a summary of the events surrounding the theft of member data of a state-chartered credit union in Washington State. The credit union had used the services of PSB, The Marketing Supersource (PSB) for mailing of marketing materials to select credit union members since mid-year 2003. Two promotional material mailings, a home-equity loan offer and credit card offer, were handled by PSB in May 2004.

A burglary of PSB's office in Lake Forest, California occurred during the night of July 8 or morning of July 9, 2004. A computer that could be easily seen from the office window was stolen. The computer was used to store member information while PSB worked on credit union promotions. PSB could not determine what information was stored on the stolen computer because it did not have a recent back-up tape of the computer; nor could it verify if PSB users had deleted the

credit union's member information after a promotion was completed. There was no evidence that the computer had been targeted for the information it contained.

On July 27, 2004, 18 days after the theft, PSB notified the credit union that member information might have been compromised. The information for 13,100 members, including names, addresses, and social security numbers, was possibly stored on the PSB computer. The Washington credit union management immediately assembled an incident response team to determine potential risks and necessary actions.

On August 2, 2004, the credit union mailed letters to all 13,100 affected members informing them of the theft and encouraging members to contact the three major credit reporting agencies and place a "Fraud Alert" with each credit reporting agency. The credit union sent members additional information to advise them to remain vigilant over the next 12 to 24 months to monitor their credit report and account activity and, if they desired, to immediately call the credit union to place a password on their account. The credit union attempted to assure members of its priority in keeping member information secure and set up a toll free number to address member concerns. As of August 17, 2004, the credit union had received over 30 letters, 5,000 phone calls, and numerous email messages from members expressing their concerns and frustrations.

On August 17, 2004, the Washington State Division of Credit Unions completed an onsite investigation of this incident. As a result, the credit union learned that its marketing department was not complying with the credit union's data security procedures. The credit union also implemented the following recommendations from the investigation:

- Maintain written contract/agreements with vendors;
- Perform and document a member information security risk assessment according to 12 C.F.R. Part 748. Update the risk assessment annually and whenever significant system changes occur. Report to the Board at least once ever year;
- Document information supplied to vendors/service providers;
- Monitor service providers;
- Require reporting from service providers to appropriately evaluate the service provider's performance and security;
- Control information supplied to service providers, ensuring that the information is managed and secured properly; and
- Encrypt electronic member information, including while in transit or in storage on networks or systems in which unauthorized individuals may have access.

There has been no evidence of fraud as a result of the member data theft.

Current Laws and NCUA Actions, Including Regulations, Guidance and Examination Procedures

The primary current federal laws governing data security for credit unions are found in the Gramm-Leach-Bliley Act of 1999 (GLBA), 15 U.S.C. §6801(b), and the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Pub. L. No. 108-159. NCUA has promulgated regulations under these laws containing requirements for credit unions to enhance data security, including Fair Credit Reporting Act regulations, 12 C.F.R. Part 717, and Security Program regulations in 12 C.F.R. Part 748.

GLBA 501b Regulations

Under the GLBA, section 501b, NCUA and other federal financial regulators were required to establish technical standards for financial institutions to meet the following objectives: one, ensuring the security and confidentiality of member records; two, protecting against anticipated threats or hazards to the security or integrity of such records; and three, protecting against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member.

Accordingly, NCUA, in consultation and coordination with the other federal financial regulators, amended its existing Security Rule, 12 C.F.R. Part 748, in 2001 to require that a federally-insured credit union's security program contain elements to meet these objectives. Appendix A of Part 748 provides guidance in developing and implementing an information security program. 66 Fed. Reg. 8152 (January 30, 2001).

Stemming from the growing number of security breaches in the financial services sector involving access to customer information, NCUA, again in consultation and coordination with the other federal financial regulators, further amended Part 748 in 2005, effective June 1, 2005. 70 Fed. Reg. 22763 (May 2, 2005). In this change, NCUA outlined its expectations that each credit union develop and maintain a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of member information. Appendix B describes the components of a response program, including procedures for notifying members about incidents of unauthorized access to or use of member information that could result in substantial harm or inconvenience to the member.

The new guidance provides that, when a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. The guidance states that if the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon

as possible. The credit union may delay the notice if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation. Under the guidance, the credit union should notify its primary regulator of a security breach involving sensitive member information, whether or not the credit union notifies its members.

Fair and Accurate Credit Transactions Act of 2003 (FACTA)

Complementing the GLBA's requirements implemented in Part 748, FACTA established new requirements and protections for credit unions and their members relating to data security. Originating with the Committee on Financial Services, FACTA amended the Fair Credit Reporting Act (FCRA) to: help consumers combat identity theft; establish national standards for the regulation of consumer report information; assist consumers in controlling the type and amount of marketing solicitations they receive; and restrict the use of sensitive medical information.

Disposal Rule

NCUA coordinated with the other federal financial regulators and issued a final rule on the Proper Disposal of Consumer Information under FACTA §216, to address the risks associated with identity theft. Under the final rule, effective December 29, 2004, federal credit unions must take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. 69 Fed. Reg. 69269, (Nov. 29, 2004); 12 C.F.R. Parts 717 and 748.

The standard for disposal is flexible to allow credit unions to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and relevant changes in technology over time. Federal credit unions are expected to implement these measures consistent with the provisions in NCUA's Guidelines for Safeguarding Member Information under Part 748, Appendix A.

The disposal rule includes specific examples of appropriate measures that would satisfy its disposal standard, both for paper and electronic records. For example, an appropriate measure would be requiring the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed. For electronic media, an appropriate measure would be requiring the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed. In addition, it would be an appropriate measure if, after due diligence, a credit union enters into and monitors compliance with a contract with another party engaged in the business of record destruction to properly dispose of the consumer information.

FACTA Regulatory Alert and Interagency Legal Opinion Letter

NCUA issued a Regulatory Alert in January 2005, 05-RA-03, Fair and Accurate Credit Transactions Act of 2003, that lists and discusses key provisions of FACTA. A copy of Regulatory Alert 05-RA-03 is attached and also available on NCUA's website at: http://www.ncua.gov/reg_alerts/2005/05-RA-03.doc. In addition, NCUA, the federal banking agencies, and the FTC jointly issued an interagency legal opinion letter offering guidance on FACTA compliance. This letter is also attached and available to the public on NCUA's website under Legal Opinion Letter 04-1140, dated November 24, 2004, http://www.ncua.gov/RegulationsOpinionsLaws/opinion_letters/2004Letters.htm.

The FACTA Regulatory Alert and Legal Opinion Letter 04-1140 both identify provisions of FACTA relating directly to handling IS&T and other data security issues, either before or after a breach has occurred. Certain FACTA provisions must be implemented by regulations or guidance adopted by federal regulators. NCUA, with other federal financial agencies, is currently actively engaged in developing guidance or rules as appropriate to implement these FACTA provisions and training credit unions and examiners.

For example, NCUA, the FTC and the federal banking agencies are participating in ongoing interagency meetings to draft a proposed Red Flags rule establishing guidelines for identifying, mitigating and preventing identity theft. FACTA §114; FCRA §615(e). The Red Flags rule will likely require credit unions to develop, implement, and monitor identity theft protection policies and procedures. The agencies also plan to issue another FACTA proposed rule to prevent identity theft on the requirement to reconcile addresses simultaneously with the proposed Red Flags rule. FACTA §315; FCRA §605(h). These regulations, once finalized, will further enhance the safeguarding of member data.

The FACTA Regulatory Alert and Legal Opinion Letter both also identify certain provisions of FACTA that became effective December 1, 2004 and do not depend on agency rulemaking. These provisions include, for example, fraud and active duty alerts, blocking of information resulting from identity theft, prevention of repollution of consumer reports, and disclosure of credit scores. Credit unions are developing compliance procedures, modifying systems, and training staff to implement the new requirements. These requirements will serve to safeguard member data and provide assistance to members whose data has been compromised or who are the victims of identity theft.

For example, the repollution provision of FACTA requires that, when reporting data to consumer reporting agencies, credit unions must have reasonable procedures to stop re-reporting data derived from identity theft transactions upon notification of identity theft by a member or consumer reporting agency (CRA). FACTA §154(a); FCRA 623(a)(6). Reasonable procedures means procedures that provide reasonable assurance that data related to an identity theft

transaction will not be reported to a consumer reporting agency, once a consumer provides notification of identity theft.

We note that acceptable procedures could vary, depending on the size and complexity of a credit union. For example, a large credit union with an automated system for reporting to CRAs should be able to flag and stop reporting identity theft transactions within hours of notification. A smaller credit union that manually submits weekly reports to the CRAs might take seven days (until the next weekly report) to update records.

While the process and procedures will vary among institutions, every credit union that reports to CRAs should take the time to establish and document, in writing, the process that will be used. In addition to strong policy and internal controls, under FACTA, NCUA has advised credit unions that during the ongoing review of internal controls, a supervisory committee member could check a sample of credit reports to confirm that identity theft information was not accidentally re-reported.

Interagency Examination Guidance and Enforcement

NCUA is currently working with a FFIEC group to draft interagency examination procedures for FACTA, prepare training modules for examination staff that will also be made available to the public, and an examiner questionnaire will be developed, based on the interagency exam procedures. By using interagency procedures, the FFIEC agencies will be able assure consistent application of FACTA provisions across all financial institutions. Should a deficiency in compliance with FACTA be noted, NCUA would work with the credit union to ensure appropriate corrections are made. NCUA will enforce FACTA like other consumer compliance regulations, such as Truth in Lending (Reg Z) and Truth in Savings (Reg DD).

Public Education and Letters to Credit Unions

In 2004, the NCUA Chairman JoAnn Johnson was appointed to the U.S. Financial Education and Literacy Commission. NCUA is a key partner with the Treasury Department on financial education initiatives, such as educating consumers on data security issues and identity theft. Credit unions also have made ongoing efforts to communicate with members about identity theft and how to protect themselves from having their identity stolen.

Moreover, FACTA imposes responsibility for the establishment and implementation of a public education campaign concerning identity theft on the FTC. NCUA and credit unions commonly refer victims of identity theft to the FTC web site, where there is a comprehensive discussion of identity theft issues. Included on the FTC website, for example, is a model summary of rights for identity theft victims. FTC developed the model summary as required under the

FCRA §609(d). During the development process, FTC solicited feedback from federal financial regulators, including NCUA. We note that the FTC FACTA manager and NCUA staff have regularly been working together, participating on lecture panels, and training credit union representatives on FACTA implementation.

In addition, NCUA has made public, through web-site posting, guidance documents addressing identity theft, which were sent to credit unions. NCUA has issued at least 30 Letters to Credit Unions related to identity theft and other IS&T data security risks, issues, and concerns, a list of which is included as an appendix. Some example of NCUA letters include:

- In May 2000, NCUA published Letter to Credit Unions 00-CU-02, Identity Theft Prevention. The Letter discussed the rising frequency of identity theft and encouraged credit unions to take precautions to deter the theft of member information. A best practices guide and reference information from the National Summit on Identity Theft were provided as enclosures.

- In September 2001, NCUA published Letter to Credit Unions 01-CU-09, Identity Theft and Pretext Calling. The Letter discussed identity theft issues and included a brochure, How to Avoid Becoming a Victim of Identity Theft, that credit unions were encouraged to share with their members.

- In August 2003, NCUA published Letter to Credit Unions 03-CU-12, Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Unions. The Letter addressed fraudulent websites used to capture sensitive personal information with the intent to commit identity fraud.

- In April 2004, NCUA published Letter to Credit Unions 04-CU-05, Fraudulent Email Schemes. The Letter discussed identity theft issues related to deceptive emails requesting sensitive personal information.

- In September 2004, NCUA published Letter to Credit Unions 04-CU-12, Phishing Guidance for Credit Unions. This Letter discussed identity theft related to phishing and enclosed the FFIEC brochure on phishing. The brochure was made available to credit unions for distribution to their membership.

In addition, we note other steps NCUA has taken:

- NCUA has issued six Regulatory Alerts and one Information Systems & Technology Advisory dealing with IS&T related regulations.
- NCUA has issues four IS&T Security Alerts.
- NCUA representatives regularly speak on IS&T related issues at credit union conferences.
- NCUA has revised its IS&T examination program (examiner questionnaires) and is currently field testing those new questionnaires.
- NCUA modified its website to include a section devoted to IS&T.

Recommendations

One continuing area of concern to NCUA is our lack of examination authority to review the operations of third party vendors that provide services, such as loan processing and Internet banking, to credit unions. The Government Accountability Office (GAO) has noted this lack of authority on at least two occasions and recommended that NCUA pursue this issue with Congress.[1] The authority currently exists for the other federal financial institution regulatory agencies and it temporarily existed for NCUA prior to expiring on December 31, 2001. The authority has been effectively used to monitor risk, including data security risk, in third party vendors. In the absence of this authority, NCUA has occasionally experienced difficulty in obtaining the full cooperation of vendors, and in obtaining key documents, such as financial statements and audit reports. Accordingly, we continue to request that Congress consider a permanent restoration of NCUA's vendor examination authority.

Also, while credit unions and other financial institutions are carefully regulated with respect to the issue of data security as a result of GLBA and FACTA, the examples in the first part of my testimony raise the question whether merchants and other parties should be subject to comparable requirements. NCUA will be happy to work with the Subcommittee as you continue to consider whether additional Congressional action is advisable to improve the existing legal framework.

Attachments

---

[1] In a GAO Audit Report dated August 1999, the GAO noted several times that the expiration of NCUA's examination authority of third party service providers for Y2K, on December 31, 2001, would limit NCUA's future ability to effectively oversee third party firms that provide Internet financial services to credit unions. The report recommended NCUA pursue retaining this authority to maintain effectiveness in ensuring the safety and soundness of credit unions' electronic financial services.

According to a more recent GAO Audit Report, GAO-04-91, "Credit Union Financial Condition," dated October 2003: "unlike the other depository institution regulators, NCUA lacks authority to review the operations of third-party vendors, which credit unions increasingly rely on to provide services such as Internet banking. However, these third-party arrangements present risks such as threats to security of information systems, availability and integrity of systems, and confidentiality of information."

[From NCUA's website http://www.ncua.gov/IST/ISTltcu.html]

Related Letters to Credit Unions

NCUA is providing the following reference material to assist you with IS&T Issues.

LETTER #	TITLE	ENCL	DATE ISSUED
04-CU-14	Risk Management of Free and Open Source Software - PDF only	PDF only	11/04
04-CU-12	Phishing Guidance for Credit Union Members - PDF or MS Word	PDF Only	09/04
04-CU-09	ATMs: Triple DES Encryption in PDF or MS Word		4/ 2004
04-CU-06	E-Mail and Internet Related Fraudulent Schemes Guidance PDF or MS Word		5/ 2004
04-CU-05	Fraudulent E-Mail Schemes		4/ 2004
03-CU-14	Computer Software Patch Management	PDF	9/ 2003
03-CU-12	Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Unions		8/ 2003
03-CU-08	Weblinking: Identifying Risks & Risk Management Techniques		4/ 2003
03-CU-07	FFIEC Release of Information Technology Examination Handbook		4/ 2003
03-CU-05	Expanded AIRES Share and Loan Layout Specifications	FAQ For Share and Loan Record Layout	4/ 2003
03-CU-03	Wireless Technology		3/ 2003
02-CU-17	e-Commerce Guide for Credit Unions		12/ 2002
02-CU-16	Protection of Credit Union Internet Addresses		12/ 2002
02-FCU-11	Tips to Safely Conduct Financial Transactions Over the Internet - An NCUA Brochure for Credit Union Members		4/2002
02-CU-13	Vendor Information Systems & Technology Reviews - Summary Results		7/2002
02-CU-08	Account Aggregation Services		4/ 2002
01-CU-21	Disaster Recovery and Business Resumption Contingency Plans		12/2001
01-CU-20	Due Diligence Over Third Party Service Providers		11/ 2001

01-CU-12	e-Commerce Insurance Considerations		10/2001
01-CU-09	Identity Theft and Pretext Calling Brochure: How to Avoid Becoming a Victim of Identity Theft		9/2001
01-CU-11	Electronic Data Security Overview		8/2001
01-CU-10	Authentication in an Electronic Banking Environment		8/ 2001
01-CU-04	Integrating Financial Services and Emerging Technology		3/ 2001
01-CU-02	Privacy of Consumer Financial Information (with Enclosure)		2/2001
00-CU-11	Risk Management of Outsourced Technology Services (with Enclosure)		12/2000
00-CU-07	NCUA's Information Systems & Technology Examination Program	Zip of Excel Files Zip of Excel Files. (Revised August 7, 2002)	10/2000
00-CU-04	Suspicious Activity Reporting (see section regarding Computer Intrusion)		6/2000
00-CU-02	Identity Theft Prevention		5/2000
97-CU-5	Interagency Statement on Retail On-line PC Banking		4/1997
97-CU-1	Automated Response System Controls		1/1997
109	Information Processing Issues		9/1989

REGULATORY ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: **January 2005** **NO: 05-RA-03**

TO: **All Federal Credit Unions**

SUBJECT: **Fair and Accurate Credit Transactions Act of 2003**

Dear Board of Directors:

The purpose of this regulatory alert is to inform credit union officials about the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Select provisions of FACTA became effective on December 1, 2004.

FACTA amends the Fair Credit Reporting Act (FCRA) to:

- help consumers combat identity theft;
- establish national standards for the regulation of consumer report information;
- assist consumers in controlling the type and amount of marketing solicitations they receive; and
- restrict the use of sensitive medical information.

FACTA helps members to combat identity theft. Consumers (members) may include initial fraud, active duty, or extended alerts on consumer reports (credit reports). The presence of these alerts imposes additional requirements on the users of credit reports. To aid members in clearing their credit reports of fraudulent identity theft transactions, credit unions must establish reasonable procedures to stop reporting on blocked information upon notification of identity theft.

FACTA provides consumers with opportunities to learn about their credit report and credit score. Credit unions must disclose a member's credit score when it is used to evaluate a residential mortgage application. Credit unions must also accompany pre-screened solicitations for credit with a disclosure that credit report information was used in making the solicitation. In addition, all consumers will be eligible to request a free annual credit report from the three nationwide consumer reporting agencies; these credits reports will become available nationwide by September 1, 2005.

FACTA also bolsters financial literacy efforts by creating a new Financial Literacy and Education Commission empowered to improve the government's financial literacy and education programs, grants, and materials.

A brief list of key FACTA provisions follows:

- When an initial fraud alert or active duty alert is shown on a credit report, a credit union generally may not extend new credit unless it has made a reasonable attempt to verify the member's identity and to confirm the validity of the request for credit. If an extended alert is shown on a credit report, no new credit can be extended unless the credit union contacts the consumer using a reasonable contact method designated by the consumer. 15 U.S.C. §1681c-1(h) and FACTA §112(a).

- Upon written request by a consumer, a credit union must provide copies of documents related to fraudulent transactions or fraudulent accounts opened in a member's name. Before information is provided, member identity must be verified and the member may be asked to show proof of an identity theft claim. 15 U.S.C. §1681g(e) and FACTA, §151(a).

- When reporting data to consumer reporting agencies, credit unions must have reasonable procedures to stop re-reporting data derived from identity theft transactions upon notification of identity theft by a member or consumer reporting agency. 15 U.S.C. §1681s-2(a) and FACTA, §154(a).

- When using a credit score to evaluate an application for a loan secured by 1 to 4 units of residential real property, a credit union must provide the applicant with a written disclosure and information about the credit score, including its numerical value. 15 U.S.C. §1681g and FACTA, §212(c).

- Credit unions must develop, implement, and maintain appropriate measures to properly dispose of consumer information derived from credit reports. These measures must be consistent with NCUA's Guidelines for Safeguarding Member Information. 15 U.S.C. §1681w and FACTA §216 and NCUA Rules and Regulations, 12 C.F.R. §717.83.

- Credit unions must notify members if they report negative information to a consumer reporting agency. This notice must occur no later than 30 days after the information is provided to the consumer reporting agency. 15 U.S.C. §1681s-2(a)(7) and FACTA, §217(a).

- When credit is offered to a member on materially less favorable terms than it is offered to a substantial portion of other members, a credit union may need to provide a risk-based pricing notification. Notification is required if the terms of the credit are material and the offer for credit is based in whole or in part on a consumer credit report. The notification must identify the consumer reporting agency providing the credit report

and provide related information. 15 U.S.C. §1681m(h) and FACTA, §311(a).

While the risk-based pricing notification requirement became effective on December 1, 2004, implementing rules and model disclosures have not yet been issued by the Federal Trade Commission (FTC) and Federal Reserve Board. When issued, the rules will set a compliance date.

Additional sections of FACTA will take effect as implementing regulations are finalized. Key sections include:

- Red flag guidelines and regulations. 15 U.S.C. §1681m(e) and FACTA, §114.
- Accuracy and Integrity Guidelines and Regulations. 15 U.S.C. §1681s-2(e) and FACTA, §312(a).
- Ability of consumer to dispute information with furnisher. 15 U.S.C. §1681s-2(a)(8) and FACTA, §312(c)
- Reconciling addresses. 15 U.S.C. §1681c(h) and FACTA, §315

Implementing regulations are being developed and published by the federal regulatory agencies. Both the NCUA website, http://www.ncua.gov/ , and the FTC website, http://www.ftc.gov/os/statutes/fcrajump.htm , contain information about FACTA. The FTC website includes a copy of FACTA, the text of the Fair Credit Reporting Act as amended by FACTA, and FTC rules that may apply to credit union service organizations.

NCUA's website includes implementing regulations for FACTA. NCUA recently adopted changes to Part 717 and Part 748 of the NCUA Rules and Regulations. These changes incorporate FACTA requirements for the disposal of consumer information. NCUA has also proposed changes to Part 717 to address affiliate marketing and the use of medical information. Final and proposed Rules and Regulations are published on the NCUA website at:
http://www.ncua.gov/RegulationsOpinionsLaws/rules_and_regs/rules_and_regs.html

If you have further questions, please contact your NCUA Regional Office.

Sincerely,

/s/

JoAnn Johnson
Chairman

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Federal Trade Commission
National Credit Union Administration
Office of the Comptroller of the Currency
Office of Thrift Supervision

November 24, 2004

Nessa Feddis
American Bankers Association
1120 Connecticut Avenue, NW
Washington, DC 20036

Subject: Fair and Accurate Credit Transactions Act of 2003 - Compliance Dates

Dear Ms. Feddis:

This letter, signed by the chief and general counsels of the Federal Deposit Insurance Corporation, Federal Reserve Board (Board), National Credit Union Administration, Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and the Acting Director of the Bureau of Consumer Protection of the Federal Trade Commission (FTC) (collectively, the Agencies), responds to your inquiry of the Agencies dated November 2, 2004. In addition to the American Bankers Association, the inquiry was submitted on behalf of the America's Community Bankers, Consumer Bankers Association, Credit Union National Association, Financial Services Roundtable, Independent Community Bankers of America, Mortgage Bankers Association, and the National Association of Federal Credit Unions (the Associations). Your inquiry seeks guidance on how the Agencies expect to apply ten provisions of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

Six of the provisions discussed in your letter must be implemented by regulations or guidance adopted by the Agencies. The provisions requiring rulemaking are:

- Red Flag Guidelines and Regulations (FACT Act § 114, FCRA § 615(e));
- Disposal of Consumer Report Information (FACT Act § 216, FCRA § 628);
- Risk-Based Pricing Notice (FACT Act § 311, FCRA § 615(h));
- Accuracy and Integrity Guidelines and Regulations (FACT Act § 312(a), FCRA § 623(e)(1));
- Ability of Consumer to Dispute Information with Furnisher (FACT Act § 312(c), FCRA § 623(a)(8)); and
- Reconciling Addresses (FACT Act § 315, FCRA § 605(h)(2)).

By their terms, sections 114, 216, 312(a) and 312(c), and the provisions of section 315 applicable to persons who have requested a consumer report require some or all of the Agencies to adopt implementing guidance or regulations. As these statutory provisions are written, the obligations of various persons flow from the guidelines and rules that are to be adopted by the designated agencies. Thus, compliance with any applicable guidance or rules cannot be determined until they are finally adopted by the Agencies. The effective date will be set forth in the guidance or rule.

Section 311 of the FACT Act, which governs risk-based pricing notices, becomes effective on December 1, 2004. The provisions of section 311 are, by their terms, enforceable only by the Federal agencies designated in section 621 of the Fair Credit Reporting Act. Joint rulemaking by the FTC and the Board will establish the parameters for compliance, including the requirements for consumer notice, and will state the date for compliance.

The designated Agencies have in several cases begun work on guidance or rules (as appropriate) to implement the provisions discussed above and hope to seek comment on various proposals in the short term. With respect to the provisions of section 216 regarding disposal of consumer information, the Agencies expect to issue a final rule by year-end that will include an effective date for compliance.

There are a number of other provisions of the FACT Act listed in your letter that do not involve the publication of implementing rules. You have asked the Agencies to indicate their willingness to take into account the implementation difficulties associated with these provisions when considering possible agency enforcement actions. In particular, you have indicated that developing and implementing systems to comply with the following provisions of the FACT Act may be complex and difficult for many institutions:

- Fraud and Active Duty Alerts (FACT Act § 112, FCRA § 605A);
- Blocking of Information Resulting from Identity Theft (FACT Act § 152, FCRA § 605B);
- Prevention of Repollution of Consumer Reports (FACT Act § 154(a)–(b), FCRA §§ 615(f), 623(a)(6)); and
- Disclosure of Credit Scores (FACT Act § 212(c), FCRA § 609(g)).

The requirements of these provisions are effective on December 1, 2004, and do not depend on agency rulemaking. As a result, the Agencies expect that covered persons will begin to comply with these provisions on that date.

The Agencies appreciate the difficulties associated with developing compliance procedures, modifying systems, and training staff to implement new requirements. Consequently, the Agencies will take into account these difficulties together with all other relevant circumstances, including the good faith efforts made by each institution to comply with these provisions when considering whether to bring enforcement actions under the FACT Act.

e Agencies note that this letter only addresses liability of regulated persons under the .CT Act and the FCRA listed above. Any obligations under other provisions of law ıuld be beyond the scope of this letter.

Sincerely,

ott Alvarez,
ıeral Counsel
ıard of Governors of the Federal
Reserve System

John E. Bowman
Chief Counsel
Office of Thrift Supervision

illiam F. Kroener, III
ıeral Counsel
ıderal Deposit Insurance Corporation

Daniel P. Stipano
Acting Chief Counsel
Office of the Comptroller of
the Currency

ydia B. Parnes
ıcting Director
ıreau of Consumer Protection
ıderal Trade Commission

Robert M. Fenner
General Counsel
National Credit Union
Administration

**PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION**

before the

**SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
COMMITTEE ON FINANCIAL SERVICES**

U.S. HOUSE OF REPRESENTATIVES

on

**ENHANCING DATA SECURITY:
THE REGULATORS' PERSPECTIVE**

May 18, 2005

I. INTRODUCTION

Mr. Chairman, I am Lydia Parnes, Director of the Bureau of Consumer Protection of the Federal Trade Commission.[1] I appreciate the opportunity to appear before you today to discuss the laws currently applicable to resellers of consumer information, commonly known as "data brokers."

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

All of this discussion takes place against the background of the threat of identity theft, a pernicious crime that harms both consumers and financial institutions. A 2003 FTC survey showed that over a one-year period nearly 10 million people – or 4.6 percent of the adult population – had discovered that they were victims of some form of identity theft.[2] As described

---

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

[2] Federal Trade Commission – Identity Theft Survey Report (Sept. 2003) (available

in this testimony, the FTC has a substantial ongoing program both to assist the victims of identity theft and to collect data to assist criminal law enforcement agencies in prosecuting the perpetrators of identity theft.

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

The information industry is large and complex and includes companies of all sizes. Some collect information from original sources, others resell data collected by others, and many do both. Some provide information only to government agencies or large companies, while others sell information to small companies or the general public.

A. Sources of Consumer Information

Data brokers obtain their information from a wide variety of sources and provide it for many different purposes. The amount and scope of information that they collect varies from company to company, and many offer a range of products tailored to different markets and uses. Some data brokers, such as consumer reporting agencies, store collected information in a database and allow access to various customers. Some data brokers may collect information for

---

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

[3] For more information on how consumer data is collected, distributed, and used, see generally General Accounting Office, *Private Sector Entities Routinely Obtain and use SSNs, and Laws Limit the Disclosure of this Information* (GAO-04-11) (2004); General Accounting Office, *SSNs Are Widely Used by Government and Could be Better Protected, Testimony Before the House Subcommittee on Social Security, Committee on Ways and Means* (GAO-02-691T) (statement of Barbara D. Bovbjerg, April 29, 2002); Federal Trade Commission, *Individual Reference Services: A Report to Congress* (December 1997) (available at http://www.ftc.gov/os/1997/12/irs.pdf). The Commission has also held two workshops on the collection and use of consumer information. An agenda, participant biographies, and transcript of "Information Flows, The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information," held on June 18, 2003, is available at http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.html. Materials related to "The Information Marketplace: Merging and Exchanging Consumer Data," held on March 13, 2001, are available at http://www.ftc.gov/bcp/workshops/infomktplace/index.html.

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

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

1. Public Record Information

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

2. Publicly-Available Information

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

---

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

3. Non-Public Information

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

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

B. Uses of Consumer Information

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

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

potential witnesses or defendants;

- Conduct marketing and market research; and
- Conduct academic research.

Government may use information collected by data brokers for:

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

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

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

III. LAWS CURRENTLY APPLICABLE TO DATA BROKERS

There is no single federal law that governs all uses or disclosures of consumer information. Rather, specific statutes and regulations may restrict disclosure of consumer information in certain contexts and require entities that maintain this information to take reasonable steps to ensure the security and integrity of that data. The FTC's efforts in this area have been based on three statutes: the Fair Credit Reporting Act ("FCRA"),[5] Title V of the Gramm-Leach-Bliley Act ("GLBA"),[6] and Section 5 of the Federal Trade Commission Act

---

[5] 15 U.S.C. §§ 1681-1681u, as amended.

[6] 15 U.S.C. §§ 6801-09.

("FTC Act").[7] Although the FCRA is one of the oldest private sector data protection laws, it was significantly expanded in 1996 and in the last Congress. The Commission is engaged in a number of rulemakings to implement the new provisions of the FCRA, many of which are directly targeted to the problem of ID Theft. The GLBA is a relatively recent law, and its implementing rule on consumer information privacy became effective in 2001. Other laws, such as the Driver's Privacy Protection Act[8] and the Health Insurance Portability and Accountability Act[9] also restrict the disclosure of certain types of information, but are not enforced by the Commission. Although these laws all relate in some way to the privacy and security of consumer information, they vary in scope, focus, and remedies. Determining which – if any – of these laws apply to a given data broker requires an examination of the source and use of the information at issue.

A. The Fair Credit Reporting Act

Although much of the FCRA focuses on maintaining the accuracy and efficiency of the credit reporting system, it also plays a role in ensuring consumer privacy.[10] The FCRA primarily prohibits the distribution of "consumer reports" by "consumer reporting agencies" ("CRAs") except for specified "permissible purposes," and requires CRAs to employ procedures to ensure that they provide consumer reports to recipients only for such purposes.

---

[7] 15 U.S.C. § 45(a).

[8] 18 U.S.C. §§ 2721-25.

[9] 42 U.S.C. §§ 1320d *et seq.*

[10] "[A] major purpose of the Act is the privacy of a consumer's credit-related data." *Trans Union Corp. v. FTC*, 81 F.3d 228, 234 (D.C. Cir. 1996).

1. Overview

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

CRAs other than credit bureaus provide many different types of consumer reports. They may report information they have compiled themselves, purchased from another CRA, or both. For example, a tenant screening service may report only the information in its files that it has

---

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

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

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

received from landlords, only a consumer report obtained from another CRA, or a combination of both its own information and resold CRA data, depending on the needs of the business and the information available. Data brokers are subject to the requirements of the FCRA only to the extent that they are providing "consumer reports."

2. "Permissible Purposes" For Disclosure of Consumer Reports

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

There is no general "law enforcement" permissible purpose for government agencies. With few exceptions, government agencies are treated like other parties – that is, they must have a permissible purpose to obtain a consumer report.[17] There are only two limited areas in which

---

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

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

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

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

the FCRA makes any special allowance for governmental entities. First, the law has always allowed such entities to obtain limited identifying information (name, address, employer) from CRAs without a "permissible purpose."[18] Second, the FCRA was amended to add express provisions permitting government use of consumer reports for counterintelligence and counter-terrorism.[19]

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

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

The Commission has implemented the general and specific requirements of this provision in a number of enforcement actions that resulted in consent orders with the major nationwide CRAs[21] and with resellers of consumer reports (businesses that purchase consumer reports from the major bureaus and resell them).[22] For example, in the early 1990s, the FTC charged that

---

[18] 15 U.S.C. § 1681f. The information a government agency may obtain under this provision does not include Social Security numbers.

[19] 15 U.S.C. §§ 1681u, 1681v.

[20] 15 U.S.C. § 1681e(a).

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

[22] *W.D.I.A.*, 117 F.T.C. 757 (1994); *CDB Infotek*, 116 F.T.C. 280 (1993); *Inter-Fact,*

resellers of consumer report information violated Section 607(a) of the FCRA when they provided consumer report information without adequately ensuring that their customers had a permissible purpose for obtaining the data.[23] In settling these charges, the resellers agreed to employ additional verification procedures, including verifying the identities and business of current and prospective subscribers, conducting periodic, unannounced audits of subscribers, and obtaining written certifications from subscribers as to the permissible purposes for which they seek to obtain consumer reports.[24] In 1996, Congress amended the FCRA to impose specific duties on resellers of consumer reports.[25]

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

B. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act imposes privacy and security obligations on "financial institutions."[26] Financial institutions are defined as businesses that are engaged in certain

---

Inc., 116 F.T.C. 294 (1993); *I.R.S.C.*, 116 F.T.C. 266 (1993) (consent agreements against resellers settling allegations of failure to adequately insure that users had permissible purposes to obtain the reports).

[23] *Id.*

[24] A press release describing the consent agreement is available at: http://www.ftc.gov/opa/predawn/F93/irsc-cdb-3.htm.

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

[26] 15 U.S.C. § 6809(3)(A).

"financial activities" described in Section 4(k) of the Bank Holding Company Act of 1956[27] and its accompanying regulations.[28] These activities include traditional banking, lending, and insurance functions, as well as other activities such as brokering loans, credit reporting, and real estate settlement services. To the extent that data brokers fall within the definition of financial institutions, they would be subject to the Act.

1. Privacy of Consumer Financial Information

In general, financial institutions are prohibited by Title V of GLBA and its implementing privacy rule[29] from disclosing nonpublic personal information to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.[30] However, GLBA provides a number of statutory exceptions under which disclosure is permitted without specific notice to the consumer. These exceptions include consumer reporting (pursuant to the FCRA), fraud prevention, law enforcement and regulatory or self-regulatory purposes, compliance with judicial process, and public safety investigations.[31] Entities that receive information under an exception to GLBA are subject to the reuse and redisclosure restrictions

---

[27] 12 U.S.C. § 1843(k).

[28] 12 C.F.R. §§ 225.28, 225.86.

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

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

[31] 15 U.S.C. § 6802(e).

under the GLBA Privacy Rule, even if those entities are not themselves financial institutions.[32] In particular, the recipients may only use and disclose the information "in the ordinary course of business to carry out the activity covered by the exception under which . . . the information [was received]."[33]

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

2. Required Safeguards for Customer Information

GLBA also requires financial institutions to implement appropriate physical, technical, and procedural safeguards to protect the security and integrity of the information they receive from customers directly or from other financial institutions.[35] The FTC's Safeguards Rule, which implements these requirements for entities under FTC jurisdiction,[36] requires financial

---

[32] 16 C.F.R. § 313.11(a).

[33] *Id.*

[34] 15 U.S.C. § 502(e)(3)(B).

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

[36] The Federal Deposit Insurance Corporation, the National Credit Union

institutions to develop a written information security plan that describes their programs to protect customer information. Given the wide variety of entities covered, the Safeguards Rule requires a plan that accounts for each entity's particular circumstances – its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. It also requires covered entities to take certain procedural steps (for example, designating appropriate personnel to oversee the security plan, conducting a risk assessment, and overseeing service providers) in implementing their plans. Since the GLBA Safeguards Rule became effective in May 2003, the Commission has brought two law enforcement actions against companies that violated the Rule by not having reasonable protections for customers' personal information.[37]

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

C. Section 5 of the FTC Act

In addition, Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or

---

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

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

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

affecting commerce."[39] Under the FTC Act, the Commission has broad jurisdiction to prevent unfair or deceptive practices by a wide variety of entities and individuals operating in commerce.

Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information.[40] To date, the Commission has brought five cases against companies for deceptive security claims, alleging that the companies made explicit or implicit promises to take reasonable steps to protect sensitive consumer information. Because they allegedly failed to take such steps, their claims were deceptive.[41] The consent orders settling these cases have required the companies to implement rigorous information security programs generally conforming to the standards set forth in the GLBA Safeguards Rule.[42]

In addition to deception, the FTC Act prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable

---

[39] 15 U.S.C. § 45(a).

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

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

[42] As the Commission has stated, an actual breach of security is not a prerequisite for enforcement under Section 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate. It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution. *See* Statement of the Federal Trade Commission Before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform (Apr. 21, 2004) (available at http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf).

by consumers nor offset by countervailing benefits to consumers or competition.[43] The Commission has used this authority to challenge a variety of injurious practices.[44]

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

D. Other Laws

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

The privacy rule under the Health Information Portability and Accountability ("HIPAA") Act allows for the disclosure of medical information (including patient records and billing statements) between entities for routine treatment, insurance, and payment purposes.[46] For non-routine disclosures, the individual must first give his or her consent. As with the DPPA, the HIPAA Privacy Rule provides a list of uses for which no consent is required before disclosure.

---

[43] 15 U.S.C. § 45(n).

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

[45] 18 U.S.C. §§ 2721-25.

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

Like the GLBA Safeguards Rule, the HIPAA Privacy Rule also requires entities under its jurisdiction to have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[47]

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

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

A. Working with Consumers

The Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft. We receive about 15,000 to 20,000 contacts per week on the hotline, or via our website or mail from victims and consumers who want to learn about how to avoid becoming a victim. The callers to the hotline receive counseling from trained personnel who provide information on prevention of identity theft, and

---

[47] 45 C.F.R. § 164.530(c).

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

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

The FTC has also taken the lead in the development and dissemination of consumer education materials. To increase awareness for consumers and provide tips for minimizing the risk of identity theft, the FTC developed a primer on identity theft, *ID Theft: What's It All About?* Together with the victim recovery guide, *Take Charge: Fighting Back Against Identity Theft*, the two publications help to educate consumers. The FTC alone has distributed more than 1.4 million copies of the *Take Charge* booklet (formerly known as *ID Theft: When Bad Things Happen To Your Good Name*) since its release in February 2000 and has recorded more than 1.8 million visits to the Web version. The FTC's consumer and business education campaign

---

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

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

includes other materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, www.consumer.gov/idtheft, which provides publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

The Commission has also developed ways to simplify the recovery process. One example is the ID Theft Affidavit, which is included in the *Take Charge* booklet and on the website. The FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. To date, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit and has recorded more than 809,000 hits to the Web version.

B. Working with Law Enforcement

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

With over 844,000 complaints, the Clearinghouse provides a picture of the nature, prevalence, and trends of the identity theft victims who submit complaints. The Commission publishes annual charts showing the prevalence of identity theft complaints by states and cities.[51] Law enforcement and policy makers use these reports to better understand identity theft.

Since the inception of the Clearinghouse, more than 1,200 law enforcement agencies have signed up for the database. Individual investigators within those agencies can access the system from their desktop computers 24 hours a day, seven days a week.

---

[51] Federal Trade Commission - National and State Trends in Fraud & Identity Theft (Feb. 2005) (available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf).

The Commission also encourages even greater use of the Clearinghouse through training seminars offered to law enforcement. Beginning in 2002, the FTC, in cooperation with the Department of Justice, the U.S. Postal Inspection Service, and the U.S. Secret Service, initiated full day identity theft training seminars for state and local law enforcement officers. To date, this group has held 18 seminars across the country. More than 2,550 officers have attended these seminars, representing over 890 different agencies. Future seminars are being planned for additional cities.

The FTC staff also developed an identity theft case referral program. The staff creates preliminary investigative reports by examining patterns of identity theft activity in the Clearinghouse. The staff then refers the investigative reports to Financial Crimes Task Forces and other law enforcers for further investigation and potential prosecution.

C. Working with Industry

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

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

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

V. CONCLUSION

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

---

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

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

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

STATEMENT OF

SANDRA L. THOMPSON
DEPUTY DIRECTOR
DIVISION OF SUPERVISON AND CONSUMER PROTECTION
FEDERAL DEPOSIT INSURANCE CORPORATION

on

"Enhancing Data Security"

before the

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT

of the

COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

May 18, 2005

Thank you Mr. Chairman, Representative Sanders, and Members of the Subcommittee. I appreciate the opportunity to present the views of the Federal Deposit Insurance Corporation on the issue of data security and protecting sensitive information. The FDIC shares the Subcommittee's concerns about the harm to consumers caused by theft of personal financial information.

Since the early 1970's, the FDIC has treated data security as a significant risk area due to its potential to disrupt bank operations, harm consumers, and undermine confidence in the banking system and economy. The failure or misuse of technology can impact the safety and soundness of an institution with sudden and severe losses, or directly harm consumers.

My testimony today will turn first to emerging trends and developing threats the FDIC is seeing in terms of security breaches. I will discuss as well the FDIC's examination programs, including existing regulations and guidance, which require banks to keep their data secure. Finally, I will discuss our outreach efforts to the industry and consumers.

Emerging Trends and Developing Threats

In its role as supervisor, the FDIC analyzes emerging cyber threats, occurrences of bank security breaches and other incidents. Data compromise and misuse are not new issues. Despite generally strong controls and practices by financial institutions, methods for stealing personal data and committing fraud with that data are continuously evolving. Due to the evolving nature

of threats, the ability to secure customer data against compromise will never be 100 percent assured.

The Internet and other technologies facilitate identity theft by offering a marketplace for the quick sale of confidential information. Not only is the Internet an integral component in nearly every facet of legitimate U.S. commerce, it also has lent its global presence to the sale and ultimate misuse of data to a degree that did not exist previously.

In addition to the Internet's far reaching beneficial attributes, the Internet has created an anonymous and lucrative channel that provides an accessible market for, and adds value to, stolen data. The Internet has made it possible to build a virtual storefront, without geographic boundaries, that criminals can use to conduct business on an increasingly larger scale.

For discussion purposes, it is useful to distinguish between information theft and information fraud. The information theft stage is targeted at consumers through schemes such as phishing, malicious software (i.e. spyware and trojans), or pharming at financial institutions through cyber intrusions from mis-configured systems or other vulnerabilities, the mishandling of data, or by insider abuse of data. Information fraud is generally targeted at financial institutions, merchants, or other servicers in order to extract value out of the information. We will discuss the most common types of attacks that we see on consumers and financial institutions.

Consumer Targeted Attacks

Malicious software on users' computers, phishing schemes, and pharming technologies are all aimed at consumers. Consumer awareness and education can mitigate or reduce some of these threats to personal information security. However, financial institutions and companies that store, transport and use consumers' information also have a responsibility in protecting that data.

Malicious Software - Consumer targeted attacks can include the delivery of spyware, keystroke loggers (programs that track and record a user's keystrokes), trojans, and other malicious code that intercept Internet access credentials (e.g. passwords) in order to commit fraud. Typically, malicious software may be bundled as a hidden component of other programs or inadvertently downloaded from the Internet. Usually, these programs are installed without the users' knowledge. In some cases, the software has even requested that users agree to the activity by including opt-in agreements. The FDIC plans to issue industry guidance advising financial institutions about potential spyware threats later this year.

Phishing - Phishing and spoofing continue to increase and now comprise over 50 percent of the incidents reported to the FDIC. Phishers have begun attacking smaller financial institutions, expanding their operations as the larger often phished banks become less fertile. The FDIC recently published a study, discussed later, that recommends financial institutions and service providers consider stronger risk based authentication strategies to reduce fraud related to compromised Internet account access credentials. An increasingly large number of banks are

introducing stronger authentication strategies for higher risk customers. The Federal Financial Institutions Examination Council (FFIEC) also has plans to release guidance related to authentication later this year.

Pharming - Pharming is a relatively new term to describe the practice of web-site redirection. Fraudsters can hijack, or steal, a company's web site name, or redirect unknowing users to phony web sites where they collect confidential data. Several industries have been attacked using pharming techniques. The FDIC issued guidance to financial institutions related to protecting and securing web site domain names as one method to prevent pharming attacks.

Financial Institution and Merchant Targeted Attacks

Credit Card Data Theft - Credit card data is a valuable commodity for criminals, as evidenced by the recent rash of publicized events. Some merchants store the credit card data collected, at the time of a sale, on their own internal computer systems. In most cases storing customer credit card data in this manner is a violation of card processing agreements. If merchant computer systems have not been adequately secured, hackers are able to connect to the credit card data stored in the vulnerable systems and copy or offload credit card information. In our experience, a compromise such as this is generally not discovered until fraudulent transactions begin to appear in cardholder accounts. Controlling the exposure is dependent upon the time it takes to verify the fraud and discover the source and extent of the compromise.

Patch Management and System Updates - In many cases, systems containing confidential data have not been updated or patched to eliminate vulnerabilities. Operating systems, software applications, Internet browsers, wireless networks, and other communication channels intended to facilitate legitimate business activities are prime targets for illegal entry as new vulnerabilities are discovered. Patches and product updates to remedy these problems are created by manufacturers and third party vendors frequently -- sometimes on a daily basis. Given the complex assortment of products required to conduct business in a largely electronic environment, an effective patch management and update program is essential for maintaining data security. A recent large scale vendor data compromise occurred because its wireless networks were not sufficiently secured. The FDIC has issued guidance to the industry on the importance of maintaining an effective computer patch management program.

Data in Transit - The loss of tapes containing sensitive information while in transport, as reported recently, is not a new threat. However, awareness that such losses can contribute to identity theft is growing. The regulators, as part of their examination process, review bank procedures for transportation and storage of critical and sensitive media. The FFIEC, in its IT Examination Handbook, recommends suggested practices for transporting backup tapes including methods for administrative, physical, and technical controls.

Financial institutions regularly transfer back-up data to secure locations using bonded and licensed courier services. There have been a number of recent instances involving the loss of tapes or other magnetic media, containing confidential customer information, while in transit between the institution and a storage facility. Encrypting data that is being transferred off site

would effectively mitigate this risk of loss but is not widely practiced due to the resources required to encrypt the information as well as the implications created by having to decrypt data as part of the recovery process associated with a primary system failure. Regulatory guidance advises financial institutions to take appropriate measures to ensure the safety of any confidential data that is being moved off site, but does not require encryption.

FDIC Identity Theft Study and FFIEC Guidance

The FDIC's concern with identity theft generally and account hijacking in particular led us to undertake a study to identify causes and possible solutions to this type of fraud. The FDIC published a study, entitled "Putting an End to Account-Hijacking Identity Theft" (Study), on December 14, 2004. The Study presents the FDIC's findings on how fraudsters get access to consumers' bank accounts and how the financial services industry and regulators can improve security to mitigate these risks. A supplement to the study will be published soon. As part of the Study, the FDIC identified several courses of action to help reduce account hijacking identity theft:

- The industry should implement more secure authentication methods for consumers using Internet banking. The current system of user IDs and passwords can easily be thwarted.
- Education programs can help consumers avoid online scams such as phishing. The federal financial regulators have published a "statement stuffer" pamphlet that financial institutions can use to help educate their customers of the risks of disclosing personal information over the Internet and to inform customers of positive computer habits such as

using anti-virus software, firewalls, and regular security updates to their systems. The FDIC also is planning for the future delivery of a consumer oriented education effort to teach consumers how to create a safer computer environment and to avoid on-line scams, such as phishing, that can lead to account hijacking and other forms of identity theft, as well as how to take action to limit liability.

- Encouraging the increased use of new technologies can help financial institutions and consumers to proactively identify and defend against phishing attacks.

- A continuing emphasis on information sharing among the financial services industry, government, and technology providers. The FDIC is hosting several identity theft symposia throughout the country to encourage and facilitate a dialogue with the industry and consumers about this issue and our findings.

As an outgrowth of our Study, the FDIC is leading a FFIEC working group to draft guidance that would set forth the regulators' expectations concerning increased security measures for Internet banking. We anticipate this guidance will be published later this year.

Examination Programs

Even before the explosive growth in the use of technology and the development of the Internet, banks and their regulators have recognized the significant importance of protecting

confidential customer data. Over the years, the entire financial sector has increasingly relied upon technology to implement core business strategies, conduct operations, create efficiencies, secure customer data, control against internal and external fraud, comply with regulations and identify new risks and opportunities. The banking regulators have included data security as a factor in the overall risk assessment of most financial institutions for over 30 years with a focus on ensuring data integrity and business continuity.

The FDIC monitors security issues in the banking industry on a regular basis through on-site examinations, regulatory reports, and news events. The FDIC works with groups such as the Finance and Banking Information Infrastructure Committee (FBIIC), the Antiphishing Working Group, other regulatory agencies, law enforcement and others to share information regarding emerging issues and coordinate our responses. While recent events in the news appear noteworthy, overall our financial institutions have strong controls. The banking regulators monitor over 8,000 financial institutions, all of which transmit or transport data on a daily basis. While a serious problem, the relative number of incidents has been small compared to the volume of transactions. At the same time, we are aware that a single incident can impact thousands of consumers. Therefore, constant vigilance is criticial.

To address the specialized nature of technology related supervision, risks, and controls in the banking industry, the FDIC regularly and routinely evaluates all of its regulated financial institutions' information security programs through our information technology (IT) examinations, as well as enforcing legal privacy requirements through our compliance examination program. As mentioned earlier, the FDIC's most direct role in ensuring cyber

security within the financial sector is through its on-site examination programs. The FDIC also conducts IT examinations of major technology service providers that support financial institutions. Through the national examination program, on-site reviews of large technology service providers are conducted on an inter-agency basis.

As you know, Congress has passed several key laws designed to protect personal information. These laws have become part of the business of banking and include the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transaction Act (FACTA), and the Fair Credit Reporting Act (FCRA). The statutes are largely implemented through regulations and interpretations and are enforced by the FDIC and other regulatory agencies through routine on-site examinations of financial institutions. Institutions that fail to comply with these laws may face enforcement actions ranging from informal agreements to civil money penalties or other administrative actions.

The FDIC takes a proactive approach to enforcing data security regulations and guidance. As part of regularly scheduled examinations, our examiners evaluate each financial institution's program for securing customer data. If that program is inadequate, the FDIC takes action regardless of whether or not there has been a compromise in data security. Depending on the severity of the findings, informal or formal enforcement action may be pursued.

For example, in a recent examination, information technology examiners identified an institution with a weak information security program that could have resulted in a breach of customer data. Weaknesses included inadequate risk assessment, inadequate policies, and

inadequate procedures for securing data. The examiners pursued a bank board resolution that included provisions to enhance the bank's risk assessment process, improve administrative controls, verify firewall controls, and develop procedures to address software and system changes, including patch management. The status of the resolution is tracked by the FDIC until each of the items is resolved by the institution. Institutions that fail to resolve problems or implement corrective action recommended by our examiners may be subject to more formal enforcement actions.

In another case, an institution operating under a memorandum of understanding (MOU) for a variety of safety and soundness and information technology issues was not correcting the problems satisfactory. A cease and desist order (Section 8(b) of the FDI Act) was issued and the institution was ordered to establish a specific timetable to conduct periodic penetration and network tests.

In response to Title V of GLBA, the FDIC implemented the *Privacy of Consumer Financial Information* regulation in Part 332 of its regulations. This privacy rule limits disclosure of nonpublic personal information by financial institutions. Subject to certain exceptions, the Privacy Rule prohibits financial institutions from disclosing a consumer's nonpublic personal information to a nonaffiliated third party unless the financial institution satisfies certain notice requirements and the consumer does not elect to prevent, or "opt out of," the disclosure.

FCRA as amended by FACTA in 2003, also contains many requirements dealing with consumer reports, and establishes new rights for identity theft victims. Newly effective requirements in the FACTA include:

- *Fraud and Active Duty Alerts* - Consumers may place alerts on their credit reports when they are victims of identity theft, or if they are members of the armed services who have been called up to active duty. Banks obtaining consumer reports that contain these alerts must take extra steps to identify the consumer to ensure that someone is not, for example, fraudulently applying for credit or opening a new account;

- *Disclosures of Information to Identity Theft Victims* - Banks must provide records to victims pertaining to applications or transactions that were the result of an alleged identity theft. This helps an identify theft victim obtain the information necessary for investigation and law enforcement; and,

- *Prevention of Re-Pollution of Reports* - Banks must ensure that transaction history related to a fraudulent account is not re-reported to consumer reporting agencies once an investigation is underway.

Moreover, the agencies are continuing to work on additional regulations to implement other provisions of the FACTA that will aid in the prevention of, or response to, cases of identity theft.

The FDIC evaluates the banks' adherence to the FCRA as part of our compliance examinations. Like the GLBA Privacy rules, interagency procedures were developed through the FFIEC for evaluating compliance with the FCRA requirements. Part of the examination process includes verifying whether banks are obtaining consumer reports only for permissible purposes. Effective management of FCRA and other programs help to ensure that financial institution employees do not obtain reports on consumers without a legitimate business reason. Also, the examinations include evaluations of banks' information sharing activities with regard to consumer report information, to determine how this information is shared and with whom, and in turn, the related consumer disclosure requirements. Under the new FACTA requirements, we have begun evaluating banks' procedures to ensure that fraud and active duty alerts are properly handled when they appear on consumer reports received by the banks. Also, the banks' procedures for providing information on fraudulent accounts and transactions to victims of identity theft are also being evaluated during compliance examinations.

In March 2001, the federal banking agencies issued *Interagency Guidelines Establishing Information Security Standards*, as required by Section 501(b) of GLBA, requiring every financial institution to have a written information security program, approved by the institution's board of directors, to protect customer information. In addition, institutions must regularly test and update their security program. The institutions must conduct a risk assessment to identify foreseeable threats and vulnerabilities that could result in the unauthorized disclosure or misuse of sensitive customer information as well as an assessment of the likelihood and potential damage that could occur to that information. There is a requirement for a system of administrative, technical and physical controls designed to mitigate the risks identified, based on

the size and complexity of the institution and with regard to how data is collected, stored, used, transmitted, protected and disposed of. An assessment of arrangements with service providers that may have access to bank customer information also must be conducted. Further, the institutions are required to have an information security training program for employees. Finally, the institution must provide its board of directors with annual reports on the state of the security program.

FDIC IT examinations are conducted in accordance with guidance established by the FFIEC for national examination programs, or through guidance developed by the FDIC for financial institution examinations. The FFIEC, in partnership with the FDIC, has published a series of Information Technology Examination Handbooks. The handbooks address objectives, standards, resources, roles and responsibilities, best practices, and examination procedures. These handbooks are available to examiners, bankers, and the public and are an excellent resource to anyone trying to establish a data security program.

Information Technology examinations address a wide range of data security issues such as:

- Information security programs and compliance with GLBA requirements;
- IT audit coverage and independent review of controls;
- Practices for development and acquisition of software and IT services;
- Administrative controls and practices, such as IT security strategies and policies and personnel controls; and,
- Operational issues such as business continuity planning and physical security.

In addition, the FDIC has issued a variety of guidance to financial institutions with respect to keeping data secure, protecting customers, and responding to breaches of data security. For example, the federal banking agencies recently issued guidelines to implement Section 216 of FACTA. The guidelines are designed to protect consumers against risks associated with identity theft by requiring financial institutions to properly dispose of consumer information. Each financial institution is required to develop and maintain, as part of its information security program, appropriate controls to ensure that it properly disposes of consumer information derived from consumer reports. These guidelines are now included as an integral part of the *Interagency Guidelines Establishing Information Security Standards*. Each bank must satisfy these guidelines by July 1, 2005, and must modify any affected contract with service providers no later than July 1, 2006.

Guidance When Data Protection Fails

The federal banking agencies issued guidance in March 2005 for financial institutions to develop and implement a *Response Program* designed to address incidents of unauthorized access to sensitive customer information. This guidance is an interpretation of Section 501(b) of GLBA and its implementing guidelines. The Guidance states that at a minimum, the response program should contain procedures for:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;

- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- Filing a timely Suspicious Activity Report (SAR) in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, and promptly notifying appropriate law enforcement authorities;
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and,
- Notifying customers in a clear manner, if the financial institution becomes aware of an incident of unauthorized access to the customer's information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or is reasonably possible to occur.

Under this Guidance, customer notice should be given in a clear and conspicuous manner and should include a description of the incident; the types of information subject to unauthorized access; measures taken by the financial institution to protect the customers from further unauthorized access; a telephone number customers can call for information and assistance; and, a reminder to customers to remain vigilant over the next 12 to 24 months, reporting any suspected identity theft incidents to the financial institution. The Guidance also encourages financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to large numbers of customers that include contact information for the reporting agencies.

Outreach

The FDIC has taken an active role in reaching large numbers of people in the financial sector to discuss cyber risks and controls. In the past three years, the FDIC has created several major outreach events:

- *Protecting the Financial Sector – A Public and Private Partnership* - The FDIC, along with other banking and financial sector regulators, are members of the FBIIC. The FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Member agencies communicate emerging issues and coordinate responses to emergency and other incidents. The FBIIC coordination effort is chaired by Department of Treasury and is chartered under the President's Working Group on Financial Markets. FBIIC coordinates with private sector organizations such as the Financial Sector Coordinating Council (FSCC) on significant information security events and incidents. The FDIC also works with Federal law enforcement agencies and regulators in both our outreach efforts and in response to specific incidents. In partnership with the FBIIC, the FDIC hosted a series of symposia examining the security of the U.S. financial sector and steps banks should take to protect themselves, including issues on cyber security. To date, the FDIC has hosted over 20 of these events around the country with over 1,000 bank executives attending.

- *FDIC Cyber Risk Management Symposium Series* - The FDIC created and hosted several outreach events to bring together government and industry to discuss current technology issues from a business perspective and a path for potential solutions. Topics have included offshore outsourcing of technology, electronic scams, incident response, information sharing, and other topics related to securing bank data.

- *Identity Theft Symposia* - The findings and recommendations of the FDIC Identity Theft study facilitated our efforts to lead the public policy and consumer education debate on identity theft. On February 11, 2005 the FDIC sponsored an identity theft symposium to coincide with the observance of National Consumer Protection Week. That symposium, attended by a standing room only group of industry representatives, consumer groups, state and local officials, academics and fellow regulators, prompted us to plan additional sessions. On May 13, 2005, the FDIC held the first of three regional symposia on this topic in Atlanta. Other symposia will follow in Los Angeles in June and Chicago in September, 2005. The symposia have brought together government, industry, law enforcement, and consumer interests to identify the scope of the identity theft problem and discuss proposed solutions. At the February 2005 symposium, the FDIC invited audience members and speakers to volunteer to participate in a consumer education focus group that will give us input on current consumer education efforts as well as consumer education needs in the area of identity theft.

- *Publications* - The FDIC frequently publishes articles on identity theft in its quarterly FDIC Consumer News. Various articles have covered cyber security from a consumer's

point of view, including how consumers can protect themselves against threats such as phishing, spyware and keystroke loggers. In addition to being available on our website, FDIC Consumer News has a circulation of over 60,000 (free of charge) and the information given is often cited by major publications, and news organizations.

Conclusion

In sum, the FDIC believes that we have the authority needed to address the risks of data security in the financial industry. No amount of legislation or regulation can completely eliminate the threat. However, we believe that our collaborative efforts with industry, the public, and our fellow regulators, will significantly minimize threats to data security. We stand ready to work with the Committee to provide assistance in any way to effectively address the elusive issues associated with data security.

Re: Need for strong identity theft legislation

May 17, 2005

Members, Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

Dear Representative:

In anticipation of tomorrow's subcommittee hearing on the security of our personal information, Consumers Union, the non-profit, independent publisher of *Consumer Reports,* would like to highlight to you the attached "Have You Heard?" Column from the June 2005 *Consumer Reports,* which addresses the critical issue of identity theft.

Identity theft is a serious crime that has become more common in recent years as we have delved further into the "information age." According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions $48 billion and consumers $5 billion. Victims pay an average of about $1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports. The personal costs can also be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

As recent scandals involving ChoicePoint, Lexis-Nexis, and others have illustrated, American consumers cannot fully protect themselves against identity theft on their own. Congress must act to protect our personal information from identity thieves. Specifically, Congress should:

- **Prevent breaches from happening in the first place.**

It is critical to impose strong requirements on information brokers to protect the information they hold and to screen and monitor the persons to whom they make that information available, and require creditors to take additional steps to verify the identity of an applicant when there is a sign of possible ID theft. In addition, Congress should act to restrict the sale, sharing, posting, display, and secondary use of Social Security numbers.

- **Require notice of breaches of sensitive information.**

Congress must impose requirements on businesses, nonprofits, and government entities to notify consumers when an unauthorized person has gained access to sensitive information pertaining to them. Consumers need prompt and proper notice, including information on what kind of data has been stolen.

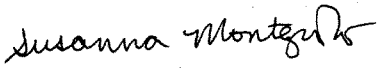
- **Ensure that victims have rights, too.**

Currently, when a company improperly breaches a consumer's sensitive information, the onus is on that consumer – the victim – to fix the problem. Congress can do much to change this and to empower consumers who are at risk for or who already are victims of identity theft, such as by strengthening the protections of the Fair and Accurate Credit Transactions Act (FACTA). FACTA can be made more effective by extending the initial fraud alert period from 90 days to one year, automatically sending consumers with a fraud alert a free credit report, and giving consumers who receive a notice of a security breach the right to an extended fraud alert.

Congress should also authorize federal, state, and private enforcement and provide funding for law enforcement to pursue multi-jurisdictional crimes promptly and effectively. Victims also need tools to fix the problem once the breach occurs – such as making sure there is a clear process for preventing identity theft and repairing credit once a breach occurs, providing for free credit monitoring, and covering the costs of fixing the problem.

Thank you for your time and consideration. If you would like more information, please do not hesitate to contact us at (202) 462-6262.

Sincerely,



Susanna Montezemolo
Policy Analyst

Chanelle Hardy
Esther Peterson Fellow

Consumer Reports®

JUNE 2005 EXPERT • INDEPENDENT • NONPROFIT

Have You Heard?

THE FIGHT AGAINST IDENTITY THEFT

"I was mugged once, years ago," one of our editorial researchers told me. "It was bad, but at least that guy had the guts to look me in the eye." This time, she'd gotten a call from her bank alerting her that someone in Oregon had just withdrawn $2,000 from her account. Since she and her husband were both at home in New York, that was very bad news.

Like many of the estimated 10 million people a year whose lives and accounts are invaded by identity thieves, our staffer had been as cautious as she could be and still be part of today's marketplace. But either her financial records were leaked or a hacker typed his or her way through the barriers protecting her account.

In either case, companies who hold sensitive personal and financial information about us, and the lawmakers who should be overseeing them, are failing to build stronger protections against the increasingly prevalent crime of ID theft. Lawmakers and regulators must work fast. Here are three things that Consumers Union, the publisher of CONSUMER REPORTS, is pushing them to do:

- Oversee information brokers, companies that collect and sell people's personal and financial data. Federal law should require them to safeguard those data, sell data only to carefully screened clients, tell consumers what's in their files, and correct mistakes promptly, since mistakes can lose you a job, a mortgage, or an insurance policy.
- Pass strong federal and state laws that require companies to notify the consumers whose personal and financial information they hold when their privacy is compromised. Now, only California residents have that protection.
- Pass laws in every state allowing consumers to "freeze" their credit-bureau files. With a security freeze in place, your credit report and score can't be given to potential new creditors unless you choose to "unlock" the file when you apply for, say, a car loan. Most businesses won't issue new credit or loans without first checking credit records. This way, thieves will hit a brick wall trying to open an account in your name.

There's no single solution to shielding consumers from the fast-changing schemes of ID thieves, so Congress should preserve the right of states to continue developing ever more sophisticated guards. For more about what CU is doing, and for what you can do to protect yourself, go to our Web sites *www.consumersunion.org/privacy* and *www.consumersunion.org/money*.

Jim Guest
President

February 28, 2006

VIA E-MAIL to fsctestimony@mail.house.gov

Committee on Financial Services
ATTN: Rodney Pearson
U.S. House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

Re: Representative Sue Kelly's Question on Securing Website Variants.

Dear Mr. Pearson:

Mr. Thomas G. Duncan requested I send you my response on behalf of the National Credit Union Administration (NCUA) to a question on securing website variants submitted by Representative Sue Kelly. The question, resulting from the May 18, 2005, Subcommittee on Financial Institutions and Consumer Credit hearing entitled "Enhancing Data Security: The Regulators' Perspective" is as follows:

> I have been told by several corporations that, when they attempted to secure all variations and possible misspellings of their web-site to prevent pharming that they were investigated by the federal government for possible anti-competitive activity. Do your agencies believe securing variants on web-sites helps protect against pharming?

NCUA has no knowledge of federal government agencies investigating for anti-competitive activity corporations attempting to secure their websites. NCUA believes securing variants on websites theoretically helps protect against pharming. Implementing such a plan, however, is not practical, reasonable, or completely effective since the universe of variants on any given web address is vast and not all these sites are illegal. We believe, however, there are several ways NCUA and credit unions can protect themselves and members from financial loss by these attacks.

NCUA is fully supportive of credit unions engaging in fraud prevention and safeguarding their websites and member information. We have been diligent in advising credit unions to protect themselves against fraud attempts, such as phishing, spoofing, and pharming, and to address them when they occur. NCUA has issued Letters to Credit Unions on these issues, including one outlining risk management control considerations on obtaining and maintaining an Internet address, NCUA Letter to Credit

Unions No. 02-CU-16, dated December 2002, entitled "Protection of Credit Union Internet Addresses," with an enclosure on "Domain Name Control Considerations," http://www.ncua.gov/letters/2002/02-CU-16.pdf. NCUA recently issued NCUA Letter to Credit Unions No. 05-CU-20, dated December 2005, entitled, "Phishing Guidance for Credit Unions and their Members," emphasizing how credit unions can educate their employees and members on how to avoid phishing and pharming scams. See http://www.ncua.gov/letters/2005/CU/05-CU-20.doc.

In addition, NCUA's Office of General Counsel operates a fraud hotline and assists and advises individual credit unions who have suffered attacks and attempted attacks by hackers and other criminals. NCUA has expended considerable resources to deal with these problems from several different angles, including, but not limited to shutting down individual websites. While we have succeeded in shutting down many of these fraudulent sites, we recognize the extremely difficult challenge of preventing the emergence of new ones and ultimately solving the underlying problem. NCUA is now concentrating on other alternatives that will seriously limit and, we hope, undermine the financial incentive to attack the credit union industry. These include aggressive education, better internal controls, and improved security.

If you need any additional information concerning this issue, please contact NCUA's Chief Information Officer Doug Verner at dverner@ncua.gov or by telephone at 703-518-6441.

Sincerely,

/s/ Robert M. Fenner

Robert M. Fenner
General Counsel

Enclosures

cc: Chief Information Officer

Response for the Record to Question in Letter to
Lydia Parnes, FTC Director of Bureau of Consumer Protection
from Committee on Financial Services
March 3, 2006

1. Question for 5-18-05 Data Security Hearing for all Witnesses: I have been told by several corporations that, when they attempted to secure all variations and possible misspellings of their web-site to prevent pharming that they were investigated by the federal government for possible anti-competitive activity. Do your agencies believe securing variants on web sites helps protect against pharming?

Pharming describes a scam that dupes a consumer's computer (or the Internet's domain name system) into redirecting traffic to a web site that masquerades as a legitimate site. Normally, when a computer user enters a web site address into his or her browser (e.g., Internet Explorer or Firefox), the browser directs the user's request to a computer that hosts the web site. When a pharming attack occurs, however, the user's computer will be misdirected to a fraudulent web site without the user's knowledge or consent.

To date, pharming attacks occur in two ways. One type of pharming attack uses a computer virus or malicious code to corrupt a host file on a user's computer. Host files convert a web site address into the number strings known as Internet Protocol addresses ("IP addresses") that the computer uses to access web sites. A computer with a compromised host file will be directed to a fake web site even if a user types in the correct web address. The second type of pharming, known as "DNS poisoning," uses a computer virus or malicious code to corrupt the domain name system ("DNS"), which is a distributed network of computers that contains indices of domain names and their corresponding IP addresses. The DNS server converts the name of a web site typed by the user into a browser into the IP address where the web site is located. Ultimately, both pharming techniques redirect a consumer to a phony web site without any visible indicators that a pharming attack has occurred.[1]

I understand that, as a defensive measure, some corporations register domain names that are similar to the name of their respective corporation to help prevent consumers from confusing

---

[1] In contrast, "phishing" uses spam, pop-up messages, and web pages that are disguised to look like an official notice from a well-known company such as a bank or an online store. The message typically tells recipients that their account information has lapsed or will lapse unless they go to a web site (which is typically a variation of the well-known web site) and provide their user name, password, or credit card information. The link for that site is in the message itself. Phishing involves tricking the consumer. Pharming, however, involves tricking the computer (or the Internet's domain name system).

misspelled web site addresses with the corporation's legitimate website.[2] While this strategy could help prevent phishing attacks by reducing the number of domain names that a scam artist could use to confuse consumers, this strategy would not prevent pharming attacks where the consumer types or clicks on a link to the actual domain name that he or she knows to be correct, not a variation of the domain.

The Commission has attacked a scheme in which a defendant registered Internet domain names that were misspellings of legitimate domain names or that incorporated transposed or inverted words or phrases. In October 2001, the FTC filed a complaint against John Zuccarini, charging that Zuccarani registered approximately 6,000 domain names which mimicked the names of companies, trademarks, service marks, and others' web sites. For example, the defendant registered 15 variations of the popular children's cartoon site, www.cartoonnetwork.com, and 41 variations on the name of teen pop star, Britney Spears. Consumers who looked for a site but misspelled its web address or inverted a term - using cartoonjoe.com, for example, rather than joecartoon.com - were taken to the defendant's sites. They then were bombarded with a rapid series of windows displaying advertisements for goods and services ranging from Internet gambling to pornography. In some cases, the legitimate web site the consumer was attempting to access also was launched, so consumers thought the hailstorm of advertisements to which they were being exposed was from a legitimate web site. The FTC alleged that the practices were unfair and deceptive, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a). On April 9, 2002, the U.S. District Court for the Eastern District of Pennsylvania in Philadelphia issued an order that permanently barred the defendant from redirecting or obstructing consumers in connection with the advertising or sale of any goods or services on the Internet, and launching the web sites of others without their permission. The order also required the defendant to pay the Commission $1,897,166 for the disgorgement of his ill-gotten gains.[3]

---

[2] Some companies are also using this defensive strategy in the context of trademark protection. The Anti CyberSquatting Act prohibits a cybersquatter's registration of domain names that are confusingly similar to the distinctive or famous trademarks or Internet domain names of another person or company. 15 U.S.C. § 1125(d).

[3] A copy of the FTC's press release and Judgment and Permanent Injunction regarding this case are available at: http://www.ftc.gov/opa/2002/05/cupcake.htm.

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, DC 20429
Office of Legislative Affairs

March 1, 2006

Honorable Sue W. Kelly
Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
House of Representatives
Washington, D.C. 20515

Dear Congresswoman Kelly:

Thank you for your question subsequent to testimony before the Subcommittee on Financial Institutions and Consumer Credit on May 18, 2005, by Sandra Thompson, currently the Acting Director of the Division of Supervision and Consumer Protection, on behalf of the Federal Deposit Insurance Corporation. Enclosed is our response to your question.

If we can provide further information, please let us know.

Sincerely,

Alice C. Goodman
Director
Office of Legislative Affairs

Enclosure

Response to a Question from
The Honorable Sue Kelly

Question: I have been told by several corporations that, when they attempted to secure all variations and possible misspellings of their web-site to prevent pharming that they were investigated by the federal government for possible anti-competitive activity. Do your agencies believe securing variants on web-sites helps protect against pharming?

Answer: Pharming refers to the redirection of an individual to an illegitimate web site through technical means. For example, an Internet banking customer, who routinely logs in to his/her online banking web site, may be redirected to an illegitimate web site instead of accessing his or her bank's web site.

Corporations should consider attempting to secure all variations and possible misspellings of their web site as part of a plan to prevent pharming. However, this practice by itself does not fully protect a corporation against all pharming schemes that attempt to attack a domain server. Registering variations of a domain name will not protect against attacks accomplished by installing malicious software directly on a user's computer.

On July 18, 2005, the FDIC issued guidance on this matter in the form of Financial Institution Letter (FIL) 64-2005 ("Pharming - Guidance on How Financial Institutions Can Protect Against Pharming Attacks"). A copy of this guidance is attached. It is also available online at http://www.fdic.gov/news/news/financial/2005/fil6405.html.

Attachment

Financial Institution Letters

"Pharming"
Guidance on How Financial Institutions Can Protect Against Pharming Attacks

FIL-64-2005
July 18, 2005

Summary: The FDIC is issuing the attached guidance to financial institutions describing the practice of "pharming," how it occurs, and potential preventive approaches. Financial institutions offering Internet banking should assess potential threats posed by pharming attacks and protect Internet domain names, which – if compromised – can heighten risks to the institutions.

Highlights:

- "Pharming" is the process of redirecting Internet domain name requests to false Web sites to collect personal information. Information collected from these sites may be used to commit fraud and identity theft.
- The attached guidance explains how pharming occurs and recommends strategies for protecting financial institution Internet domain names from a successful pharming attack.
- The effectiveness of an insured institution's Internet domain name protection program should be addressed in periodic risk assessments and status reports presented to the institution's board of directors.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer

Related Topics:
GLBA, Section 501b
FIL-77-2000, Bank Technology Bulletin, November 2000
FIL-27-2004, Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraud, March 2004
FFIEC Information Security Handbook, Issued November 2003
Interagency Informational Brochure on Phishing Scams, Contained in FIL-113-2004, Issued September 13, 2004
Putting an End to Account- Hijacking Identity Theft Study, Issued December 2004

Attachment:
Guidance on How Financial Institutions Can Protect Against Pharming Attacks

Contact:
Senior Technology Specialist Robert D. Lee at Rolee@fdic.gov or (202) 898-3688.

Printable Format:
FIL-64-2005 - PDF 48k (PDF Help)

Note:
FDIC Financial Institution Letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2005/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC FILs may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342 or 202-416-6940).

Last Updated 07/18/2005 communications@fdic.gov

Financial Institution Letters

Guidance on How Financial InstitutionsCan Protect Against Pharming Attacks

The Federal Deposit Insurance Corporation (FDIC) has prepared guidance for financial institutions on the risks posed by "pharming" and strategies that can help mitigate those risks. "Pharming" is the practice of redirecting Internet domain name requests to false Web sites in order to capture personal information, which may later be used to commit fraud and identity theft. While pharming is similar to phishing in that both practices try to entice individuals to enter personal information on a fraudulent Web site, they differ in how they direct individuals to that site:

- **Phishing** – as in fishing for confidential information – is a scam that encompasses fraudulently obtaining and using an individual's personal or financial information. In a typical case, the consumer receives an e-mail appearing to originate from a financial institution, government agency or other entity that requests personal or financial information. The e-mail often indicates that the consumer should provide immediate attention to the situation described by clicking on a link. The provided link appears to be the Web site of the financial institution, government agency or other entity. However, in "phishing" scams, the link is not to an official Web site, but rather to a phony Web site. Once inside that Web site, the consumer may be asked to provide a Social Security number, account numbers, passwords or other information used to identify the consumer, such as the maiden name of the consumer's mother or the consumer's place of birth. When the consumer provides the information, those perpetrating the fraud can begin to access consumer accounts or assume the person's identity.
- **Pharming** refers to the redirection of an individual to an illegitimate Web site through technical means. For example, an Internet banking customer, who routinely logs in to his online banking Web site, may be redirected to an illegitimate Web instead of accessing his or her bank's Web site.

Pharming can occur in four different ways:

- **Static domain name spoofing:** The "pharmer" (the person or entity committing the fraud) attempts to take advantage of slight misspellings in domain names to trick users into inadvertently visiting the pharmer's Web site. For example, a pharmer may redirect a user to **anybnk.com** instead of **anybank.com**, the site the user intended to access.
- **Malicious software (Malware):** Viruses and "Trojans" (latent malicious code or devices that secretly capture data) on a consumer's personal computer may intercept the user's request to visit a particular site, such as **anybank.com**, and redirect the user to the site that the pharmer has set up.
- **Domain hijacking:** A hacker may steal or hijack a company's legitimate Web site, allowing the hacker to redirect all legitimate Internet traffic to an illegitimate site. Domain names generally can be hijacked in two ways:
  - **Domain slamming:** By submitting domain transfer requests, a domain is switched from one registrar to another. The account holder at the new registrar can alter routing instructions to point to a different, illegitimate server.
  - **Domain expiration:** Domain names are leased for fixed periods. Failure to manage the leasing process properly could result in a legitimate ownership transfer. In this instance, trade name laws usually must be invoked to recover lost domains.

- **DNS poisoning:** The most dangerous instance of pharming may be domain name server (DNS) poisoning. Domain name servers are similar to Internet road map guides. When an individual enters www.anybank.com into his or her browser, Domain Name Servers on the Internet translate the phrase **anybank.com** into an Internet protocol (IP) address, which provides routing directions. After the DNS server provides this address information, the user's connection request is routed to **anybank.com**. Local DNS servers can be "poisoned" to send users to a Web site other than the one that was requested. This poisoning can occur as a result of misconfiguration, network vulnerabilities or Malware installed on the server.

  There are 13 root DNS servers for the entire Internet, which are closely protected and controlled. Most requests are directed by the local DNS server before they reach a root DNS server. However, if a hacker were to penetrate one or more of these root servers, the Internet could be severely compromised.

Detection and Prevention
Consumers and businesses can take several steps to prevent pharming attacks:

- **Digital certificates:** Legitimate Web servers can differentiate themselves from illegitimate sites by using digital certificates; Web sites using certificate authentication are more difficult to spoof. Consumers can use the certificate as a tool to determine whether a site is trustworthy.
- **Domain name management:** Financial institutions should diligently manage domain names by ensuring that the domain names are renewed in a timely manner. Institutions also should investigate the possibility of registering similar domain names. In addition, many registrars offer domain locks[1] to prevent unauthorized domain slamming. For more information about managing domain names, refer to FIL-77-2000, which includes a *Bank Technology Bulletin* informing banks about the risks related to poor domain name management and recommended best practices.
- **DNS poisoning:** Insured financial institutions should investigate anomalies about their Web site to ensure that DNS poisoning attacks are addressed promptly. For example, if **Anybank**'s domain was hijacked, it would immediately stop receiving normal Internet-related requests. The drop in Internet traffic should alert technology staff at **Anybank** to the problem, which the staff should then investigate.
- **Consumer education:** The financial institution should recommend Internet banking customers install current versions of virus detection software, firewalls and spyware scanning tools to reduce computer infections, and should stress the importance of regularly updating these tools to combat new threats. The institution also should educate consumers about how to know when they are connected to a trusted site instead of a spoofed site.

Conclusion
Financial institution domain names are critical and valuable financial institution property that should be protected. Financial institutions and their Internet banking customers may be vulnerable to data and financial loss if domain names are misused or otherwise redirected. Practices to monitor and protect domain names should be regularly reviewed and updated as part of a financial institution's information security program.

---

[1] Generally, if someone wants to transfer a domain name, he or she would make the request at the registrar's Web site. The domain may then be intentionally or unintentionally transferred to the person making the request. If the name is locked, the request is automatically denied. If the owner of the domain name wishes to transfer the name, he or she would have to unlock the domain name before proceeding.

Last Updated 07/18/2005 communications@fdic.gov

Written statement of

GAIL HILLEBRAND

Senior Attorney
Consumers Union
(415) 431-6747
hillga@consumer.org

Entitled

Identity for Sale?
Protecting Consumers from Identity Theft

House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit
May 18, 2005

SUMMARY

Consumers Union,[1] the non-profit, independent publisher of *Consumer Reports,* believes that the recent announcements by ChoicePoint, Lexis-Nexis, and many others about the lack of security of our most personal information underscores the need for Congress and the states to act to protect consumers from identity theft.

Identity theft is a serious crime that has become more common in recent years as we have delved further into the "information age." According to the Federal Trade commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions $48 billion and consumers $5 billion. Victims pay an average of $1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports. The personal costs can also be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

And as ongoing scandals involving ChoicePoint, Lexis-Nexis, and others point to, American consumers cannot fully protect themselves against identity theft on their own. Even consumers who do "everything right," such as paying their bills on time and holding tight to personal information such as Social Security numbers and dates of birth, can become victim through no fault of their own because the companies who profit from this information have lax security standards.

Therefore, Congress and the states must enact new obligations grounded in Fair Information Practices[2] on those who hold, use, sell, or profit from private information about consumers. In this context, Fair Information Practices would reduce the collection of unnecessary information, restrict the use of information to the purpose for which it was initially provided, require that information be

---

[1] Consumers Union is a non-profit membership organization chartered in 1936 under the laws of the state of New York to provide consumers with information, education and counsel about goods, services, health and personal finance, and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports,* its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with more than four million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

[2] The Code of Fair Information Practices was developed by the Health, Education, and Welfare Advisory Committee on Automated Data Systems, in a report released two decades ago. The Electronic Privacy Information Center has described the Code as based on these five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Electronic Privacy Information Center, http://www.epic.org/privacy/consumer/code_fair_info.html.

kept secure, require rigorous screening of the purposes asserted by persons attempting to gain access to that information, and provide for full access to and correction of information held.

Consumers Union recommends that lawmakers do the following:

- **Require notice of all security breaches:** Impose requirements on businesses, nonprofits, and government entities to notify consumers when an unauthorized person has gained access to sensitive information pertaining to them. Consumers Union supports S. 751, by Senator Dianne Feinstein, which would put these requirements in place. We also believe that S. 768, introduced by Senator Charles Schumer and Senator Bill Nelson, will make an excellent notice of breach law.

- **Require and monitor security:** Impose strong requirements on information brokers to protect the information they hold and to screen and monitor the persons to whom they make that information available. S. 768, as well as S. 500 and H.R. 1080, introduced by Senator Bill Nelson and Representative Ed Markey, respectively, would direct the Federal Trade Commission to develop such standards and oversee compliance with them.

- **Give consumers access to and a right to correct information:** Give individuals rights to see, dispute, and correct information held by information brokers. This is also addressed in the Schumer/Nelson and Nelson/Markey bills.

- **Protect SSNs:** Restrict the sale, collection, use, sharing, posting, display, and secondary use of Social Security numbers.

- **Require more care from creditors:** Require creditors to take additional steps to verify the identity of an applicant when there is an indicator of possible ID theft.

- **Grant individuals control over their sensitive information:** Give individuals rights to control who collects – and who sees – sensitive information about them.

- **Restrict secondary use of sensitive information:** Restrict the use of sensitive personal information for purposes other than the purposes for which it was collected or other uses to which the consumer affirmatively consents.

- **Fix FACTA:** A consumer should be able to access more of his or her Fair and Accurate Credit Transactions Act (FACTA) rights, such as the extended fraud alert, *before* becoming an ID theft victim. Further, one of the key FACTA rights is tied to a police report, which victims still report difficulty in getting and using.

- **Create strong and broadly-based enforcement:** Authorize federal, state, local, and private enforcement of all of these obligations.

- **Recognize the role of states:** States have pioneered responses to new forms of identity crime and risks to personal privacy. Congress should not inhibit states from putting in place additional identity theft and privacy safeguards.

- **Provide resources and tools for law enforcement:** Provide funding for law enforcement to pursue multi-jurisdictional crimes promptly and effectively. Law enforcement also may need new tools to promote prompt cooperation from the Social Security Administration and private creditors in connection with identity theft investigations.

After a very brief discussion of the problem of identity theft, each recommendation is discussed.

The problem of identity theft is large and growing

Current law simply has not protected consumers from identity theft. The numbers tell part of the story:

- According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the last five years, costing businesses and financial institutions $48 billion, plus another $5 billion in costs to consumers.
- Commentator Bob Sullivan has estimated that information concerning two million consumers is involved in the security breaches announced over just the six weeks ending April 6, 2005. *Is Your Personal Data Next?: Rash of Data Heists Points to Fundamental ID Theft Problem*, http://msnbc.msn.com/id/7358558
- Based on a report to the FTC in 2003 which concluded that there were nearly 10 million identity theft victims each year, Consumers Union estimates that every minute 19 more Americans become victims of ID theft.

These numbers can't begin to describe the stress, financial uncertainty, lost work-time productivity and lost family time identity theft victims experience. Even financially responsible people who routinely pay their bills on time can find themselves in a land of debt collector calls, ruined credit and lost opportunities for jobs, apartments, and prime credit. With more and more scandals coming out every week, the time has come for Congress to act to protect the security of our personal information.

Recommendations

Notification:

Notice of security breaches of information, whether held in computerized or paper form, are the beginning, not the end, of a series of steps needed to begin to resolve the fundamental conundrum of the U.S. information U.S. society: collecting information generates revenues or efficiencies for the holder of the information but can pose a risk of harm to the persons whose economic and personal lives are described by that information.

The first principle of Fair Information Practices is that there be no collection of data about individuals whose very existence is a secret from those individuals. A corollary of this must be that when the security of a collection of data containing sensitive information about an individual is breached, that breach cannot be kept secret from the individual. Recognizing the breadth of the information that business, government, and others hold about individuals, Consumers Union recommends a notice of breach requirement that is strong yet covers only "sensitive" personal information, including account numbers, numbers commonly used as identifiers for credit and similar purposes, biometric information, and similar information. This sensitive information could open the door to future identity theft, so it is vital that people know when this information has been breached.

Consumers Union supports a notice-of-breach law which does the following:

- Covers paper and computerized data
- Covers government and privately-held information

- Does not except encrypted data
- Does not except regulated entities
- Has no loopholes, sometimes called "safe harbors"
- Is triggered by the acquisition of information by an unauthorized person
- Requires that any law enforcement waiting period must be requested in writing and be based on a serious impediment to the investigation
- Gives consumers who receive a notice of breach access to the federal right to place an extended fraud alert.

Consumers Union supports S. 751, which contains these elements. S. 768 contains most, but not all, of these elements and in certain other respects provides additional protections.

Three of these elements are of special importance: covering all breaches without exceptions or special weaker rules for particular industries, covering data contained on paper as well as on computer, and covering data whether or not it is encrypted. First, a "one rule for all breaches" is the only way to ensure that the notice is sufficiently timely to be useful by the consumer for prevention of harm. "One rule for all" is also the only rule that can avoid a factual morass which could make it impossible to determine if a breach notice should have been given. By contrast, a weak notice recommendation such as the one contained in the guidance issued by the bank regulatory agencies[3] cannot create a strong marketplace incentive to invest the time, money, and top-level executive attention to reduce or eliminate, future breaches.

Second, unauthorized access to paper records, such as hospital charts or employee personnel files, are just as likely to expose an individual to a risk of identity theft as theft of computer files. Third, encryption doesn't protect information from insider theft, and the forms of encryption vary widely in their effectiveness. Further, even the most effective form of encryption can quickly become worthless if it is not adapted to keep up with changes in technology and with new tools developed by criminals.

A requirement to give notice of a security breach elevates the issue of information security inside a company. A requirement for swift, no-exemption notice of security breaches should create reputational and other marketplace incentives for those who hold sensitive consumer information to improve their internal security practices. For example, California's security breach law has led to improved data security in at least two cases. According to news reports, after giving its third notice of security breach in fifteen months, Wells Fargo Bank ordered a comprehensive review of all its information handling practices. The column quoted a memo from Wells Fargo's CEO stating in part: "The results have been enlightening and demonstrate a need for additional study, remediation

[3] That weak recommendation allows a financial institution to decide whether or not its customers need to know about a breach, and the explanatory material even states that it can reach a conclusion that notice is unnecessary without making a full investigation. *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 12 CFR Part 30, 12 CFR Parts 208 and 225, 12 CFR Part 364, 12 CFR Parts 568 and 570. Other reasons why those guidelines are insufficient to substitute for a statutory requirement to give notice include that they do not apply to non-customers about whom the financial institution has sensitive data, that there is no direct or express penalty for violation of the guideline,, and that their case-by-case approach will make it extremely hard to determine in which circumstances the guidance actually recommends notice to consumers, complicating the process of showing that an obligation was unmet.

and oversight... .Approximately 70 percent of our remote data has some measure of security exposure as stored and managed today."[4]

In another example, UC Berkeley Chancellor Robert Bigeneau announced plans to hire an outside auditor to examine data gathering, retention, and security, telling employees: "I insist that we safeguard the personal information we are given as if it were our own."[5] This announcement followed the second announced breach of the security of data held by the University in six months, this one involving 100,000 people.[6]

In the Sarbanes-Oxley Act, Congress recognized the importance of the "tone at the top," and for that reason took steps to require the corporate boards and CEOs work to improve the quality and accuracy of audited financial statements. A strong, clear notice of security breach law, without exceptions, could similarly focus the attention of top management on information security— creating an incentive for a "tone at the top" to take steps to minimize or eliminate security breaches.

Security:

Consumers Union supports S. 500 and H.R. 1080, introduced by Senator Bill Nelson and Representative Ed Markey, respectively. These measures would direct the Federal Trade Commission (FTC)to promulgate strong standards for information security and a strong obligation to screen customers, both initially and with respect to how those customers further protect the information from unauthorized use. They also provide for ongoing compliance monitoring by the FTC. S. 768, the Schumer/Nelson bill, contains similar provisions.

If Congress wanted to take even stronger steps with respect to information brokers, it could require information brokers to undergo annual audits, paid for by the broker and performed by an independent auditor retained by the FTC, with specific authority in the FTC to require corrective action for security and customer screening weaknesses identified in the audit, as well as allowing the FTC to specify particular aspects of information security that should be included in each such audit.

Any federal information broker law must require strong protections in specific aspects of information security, as well as imposing a broad requirement that security in fact be effective and be monitored for ongoing effectiveness. Congress must determine the balance between the public interest in the protection of data and the business interest in the business of information brokering. Security breaches and the effects on consumers of the ongoing maintenance of files on most Americans by information brokers are issues too important to be delegated in full to any regulatory agency.

Access and Correction:

Two of the basic Fair Information Practices are the right to see and the right to correct information held about the consumer. S. 768, S. 500, and H.R. 1080 all address these issues. While the Fair Credit Reporting Act (FCRA) allows consumers to see and correct their credit reports, as defined by

---

[4] D. Lazarus, "Wells Boss Frets Over Security," *S.F. Chronicle*, Feb. 23, 2005. http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/02/23/BUGBHBFCR11.DTL

[5] "Cal Laptop Security Put Under Microscope," April 6, 2005, *Inside Bay Area*, http://www.insidebayarea.com/searchresults/ci_2642564.

[6] Opinion Page, *Oakland Tribune*, April 5, 2005.

FCRA, consumers currently have no legal right to see the whole file held on them by an information broker such as ChoicePoint and Lexis-Nexis, even though the information in that file may have a profound effect on the consumer. There is also lack of clarity about what a consumer will be able to see even under the FCRA if the information broker has not yet made a report to a potential employer or landlord about that consumer.[7]

Because the uses of information held by data brokers continue to grow and change, affecting consumers in myriad ways, consumers must be given the legal right to see all of the information data brokers hold on them, and to seek and win prompt correction of that information if it is in error.

Protection for SSNs:

The Social Security number (SSN) has become a de facto national identifier in a number of U.S. industries dealing with consumers. Some proposals for reform have emphasized consent to the use, sale, sharing or posting of Social Security numbers. Consumers Union believes that a consent approach will be less effective than a set of rules designed to reduce the collection and use of sensitive consumer information.

Take, for example, an analogy from the recycling mantra: "Reduce, reuse, recycle." Just as public policy to promote recycling first starts with "reducing" the use of materials that could end up in a landfill, so protection of sensitive personal information should begin with reduction in the collection and use of such information. Restrictions on the use of the Social Security number must begin with restricting the initial collection of this number to only those transactions where the Social Security number is not only necessary, but also essential to facilitating the transaction requested by the consumer. The same is true for other identifying numbers or information that may be called upon as Social Security numbers are relied upon less.

Consumers Union endorses these basic principles for an approach to Social Security numbers:

- Ban collection and use of SSNs by private entities or by government except where necessary to a transaction and there is no alternative identifier which will suffice.
- Ban sale, posting, or display of SSNs, including no sale of credit header information containing SSNs. There is no legitimate reason to post or display individuals' Social Security numbers to the public.
- Ban sharing of SSNs, including between affiliates.
- Ban secondary use of SSNs, including within the company which collected them.
- Out of the envelope: ban printing or encoding of SSNs on government and private checks, statements, and the like
- Out of the wallet: ban use of the SSN for government or private identifier, except for Social Security purposes. This includes banning the use of the SSN, or a variation or part of it, for government and private programs such as Medicare, health insurance, driver's licenses or driver's records, and military, student, or employee identification. Any provision banning the printing of SSNs on identifying cards should also prohibit encoding the same information on the card.
- Public records containing SSNs must be redacted before posting.

[7] Testimony of Evan Hendricks, Editor/Publisher, *Privacy Times* before the Senate Banking Committee, March 15, 2005, http://banking.senate.gov/files/hendricks.pdf.

- There should be no exceptions for regulated entities.
- There should be No exception for business-to-business use of SSNs.

Congress should also consider whether to impose the same type of "responsibility requirements" on the collection, sale, use, sharing, display and posting of other information that could easily evolve into a substitute "national identifier," including drivers license number, state non-driver information number, biometric information and cell phone numbers.

Creditor identity theft prevention obligations:

Information is stolen because it is valuable. A key part of that value is the ability to use the information to gain credit in someone else's name. That value exists only because credit granting institutions do not check the identity of applicants carefully enough to discover identity thieves before credit is granted.

Financial institutions and other users of consumer credit reports and credit scores should be obligated to take affirmative steps to establish contact with the consumer before giving credit or allowing access to an account when there is an indicator of possible false application, account takeover or unauthorized use. The news reports of the credit card issued to Clifford J. Dawg, while humorous, illustrate a real problem— creditor eagerness to issue credit spurs inadequate review of the identity of the applicant.[8] When the applicant is a dog, this might seem funny, but when the applicant is a thief, there are serious consequences for the integrity of the credit reporting system and for the consumer whose good name is being ruined.

As new identifiers evolve, criminals will seek to gain access to and use those new identifiers. Thus, any approach to attacking identity theft must also impose obligations on those who make that theft possible – those who grant credit, goods, or services to imposters without taking careful steps to determine with whom they are dealing.

At minimum, creditors should be required to actually contact the applicant to verify that he or she is the true source of an application for credit when certain triggering events occur. The triggering events should include any of the following circumstances:

- Incomplete match on Social Security number
- Address mismatch between application and credit file
- Erroneous or missing date of birth in application
- Misspellings of name or other material information in application
- Other indicators as practices change

Under FACTA, the FTC and the federal financial institution regulators are charged with developing a set of red flag "guidelines" to "identify possible risks" to customers or to the financial institution. However, FACTA stops with the identification of risks. It does not require that financial institutions do anything to address those risks once identified through the not-yet-released guidelines. The presence of a factor identified in the guidelines does not trigger a statutory

[8] Both the news stories about Clifford J. Dawg and a thoughtful analysis of the larger problem of too lax identification standards applied by creditors is found in C. Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, in *Securing Privacy in the Information Age* (forthcoming from Stanford University Press), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=650162.

obligation to take more care in determining the true identity of the applicant before granting credit. Congress should impose a plain, enforceable obligation for creditors to contact the consumer to verify that he or she has in fact sought credit when certain indicators of potential identity theft are present.

Control for consumers over affiliate-sharing, use of information, use of credit reports and credit scores:

Consumers are caught between the growth in the collection and secondary use of information about them on the one hand and the increasing sophistication of criminals in exploiting weaknesses in how that information is stored, transported, sold by brokers, shared between affiliates, and used to access credit files and credit scores.

Identity theft has been fueled in part by information-sharing between and within companies, the existence of databases that consumers don't know about and can't stop their information from being part of, the secondary use of information, and the granting of credit based on a check of the consumer credit file or credit score without efforts to verify the identity of the applicant.[9] Consumers Union has consistently supported federal and state efforts to give consumers the legal right to stop the sharing of their sensitive personal information among affiliates. Finally, it is essential to stopping the spread of numbers that serve as consumer identifiers that Congress and the states impose strong restrictions on the use of sensitive personal information for purposes other than the purpose for which the consumer originally provided that information.

Fix FACTA:

FACTA has made some things more difficult for identity theft victims, according to information provided to Consumers Union by nonprofits and professionals who assist identity theft victims. Moreover, FACTA gives only limited rights to those who have not yet become victims of identity theft, and FACTA fails to offer a pure prevention tool for all consumers. A consumer who asserts in good faith that he or she is about to become a victim of identity theft gets one right under FACTA— the right to place, or renew, a 90 day fraud alert. However, this type of alert places lower obligations on the potential creditor than the extended alert, which is restricted only to identity theft victims.

A consumer should be able to access more of his or her FACTA rights, such as the extended fraud alert, before becoming an identity theft victim. One key FACTA right is tied to a police report, which victims still report difficulty in getting and using.

Here are some key ways to make FACTA work for victims:

- Initial fraud alert should be one year, not 90 days
- Extended alert and other victims' rights, other than blocking of information, should be available to all identity theft victims who fill out the FTC ID theft affidavit under penalty of perjury
- Business records should be available to any consumer who fills out the FTC ID theft affidavit under penalty of perjury

[9] Secondary use is use for a purpose other than the purpose for which the consumer gave the information.

- Consumers who receive a notice of security breach should be entitled to place an extended fraud alert
- Consumers who place a fraud alert have the right under FACTA to a free credit report, but this should be made automatic.

There is also work to do outside of FACTA, including work to develop a police report that could be given to victims that is sufficiently similar, if not uniform, across jurisdictions, so that the victim does not find creditors or businesses in another jurisdiction refusing to accept a police report from the victim's home jurisdiction.

Congress must encourage the states to continue to pioneer prompt responses to identity crime:

Virtually every idea on the table today in the national debate about stemming identity theft and protecting consumer privacy comes from legislation already enacted by a state. Congress must not cut off this source of progress and innovation. Instead, any identity theft and consumer privacy legislation in Congress should expressly permit states to continue to enact new rights, obligations, and remedies in connection with identity theft and consumer privacy to the full extent that the state requirements are not inconsistent with the specific requirements of federal law.

Criminals will always be more fast-acting, and fast-adapting, than the federal government. An important response to this reality is to permit, and indeed encourage, state legislatures to continue to act in the areas of identity theft and consumer privacy. Fast-acting states can respond to emerging practices that can harm consumers while those practices are still regional, before they spread nationwide. For example, California enacted its notice of security breach law and other significant identity theft protections because identity theft was a significant problem in California well before it became, or at least was recognized as, a national crime wave.

Identity theft illustrates how much quicker states act on consumer issues than Congress. According to numbers released by the FTC, there were 9.9 million annual U.S. victims of identity theft in the year before Congress adopted the relatively modest rights for identity theft victims found in FACTA. The identity theft provisions adopted by Congress in FACTA were modeled on laws already enacted in states such as California, Connecticut, Louisiana, Texas, and Virginia.[10]

Strong and broadly-based enforcement:

Consumers need effective enforcement of those obligations and restrictions Congress imposes in response to the increasing threats to consumer privacy, and of the growth of identity

---

[10] See California Civil Code §§ 1785.11.1, 1785.11.2, 1785,16.1; Conn. SB 688 §9(d), (e), Conn. Gen. Stats. § 36a-699; IL Re. Stat. Ch. 505 § 2MM; LA Rev. Stat. §§ 9:3568B.1, 9:3568C, 9:3568D, 9:3571.1 (H)-(L); Tex. Bus. & Comm. Code §§ 20.01(7), 20.031, 20.034-039, 20.04; VA Code §§ 18.2-186.31:E.

The role of the states has also been important in financial issues unrelated to identity theft. Here are two examples. In 1986, California required that specific information be included in credit card solicitations with enactment of the then-titled Areias-Robbins Credit Card Full Disclosure Act of 1986. That statute required that every credit card solicitation to contain a chart showing the interest rate, grace period, and annual fee. 1986 Cal. Stats., Ch. 1397, codified at California Civil Code § 1748.11. Two years later, Congress chose to adopt the same concept in the Federal Fair Credit and Charge Card Disclosure Act (FCCCDA), setting standards for credit card solicitations, applications and renewals. P. L. 100-583, 102 Stat. 2960 (Nov. 1, 1988), codified in part at 15 U.S.C. §§ 1637(c) and 1610(e). The implementing changes to federal Regulation Z included a model form for the federal disclosure box which is quite similar to the form required under the pioneering California statute. 54 Fed. Reg. 13855, Appendix G.

theft. A diversity of approaches strengthens enforcement. Each statutory obligation imposed by Congress should be enforceable by federal agencies, the federal law enforcement structure with the Attorney General and U.S. Attorneys, and State Attorneys General. Where a state is structured so that part of the job of protecting the public devolves to a local entity, such as a District Attorney or City Attorney, those local entities also should be empowered to enforce anti-identity theft and privacy measures in local civil or, where appropriate, criminal courts.

There is also a role for a private right of action. It is an unfortunate reality in identity theft is that law enforcement resources are slim relative to the size of the problem. This makes it particularly important that individuals be given a private right of action to enforce the obligations owed to them by others who hold their information. A private right of action is an important part of any enforcement matrix.

Money and tools for law enforcement:

Even if all the recommended steps are taken, U.S. consumers will still need vigorous, well-funded law enforcement. At a meeting convened by Senator Feinstein which included some twenty representatives of law enforcement, including police departments, sheriffs, and District Attorneys, law enforcement uniformly proposed that they be given tools to more effectively investigate identity theft. Law enforcement costs money, and the law enforcers noted that the multi-jurisdictional nature of identify theft increases the costs and time, it takes to investigate these crimes.

Law enforcers in California and Oregon have noted a strong link between identity theft crime and methamphetamine. The Riverside County Sheriff noted at a March 29, 2005 event that when drug officers close a methamphetamine lab, they often find boxes of fake identification ready for use in identity theft. The drug team has closed the lab; without funding for training and ongoing officer time, there may be no investigation of those boxes of identities.

To prove a charge of attempted identity theft, a prosecutor may need to prove that the real person holding a particular driver's license number, credit or debit card number, or Social Security number is different from the holder of the fake ID. Doing this may require the cooperation of a state Department of Motor Vehicles, a financial institution, or the Social Security Administration. The public meetings of the California High Tech Crimes Advisory Committee have including discussion of the difficulties and time delays law enforcement investigators encounter in trying to obtain this cooperation. Congress should work with law enforcement and groups representing interest in civil liberties to craft a solution to verifying victim identity that will facilitate investigation of identity theft without infringing on the individual privacy of identity theft victims and other individuals.

Law enforcement may have more specific proposals to enhance their effectiveness in fighting identity theft. Consumers Union generally supports:

- Funding for regional identity theft law enforcement task forces in highest areas of concentration of victims, and of identity thieves
- Funding for investigation and prosecution
- An obligation on creditors, financial institutions, and the Social Security Administration to provide information about suspected theft-related accounts or numbers to local, state, and federal law enforcement after a simple, well designed, request process

Consumers Union believes that the time has come for both Congress and state legislatures to act to stem identity theft through strong and meaningful requirements to tell consumers of security breaches; strong and detailed security standards and oversight for information brokers, reining in the use of Social Security numbers, increased control for consumers over the uses of their information, and obligations on creditors to end their role in facilitating identity theft through lack of care in credit granting. This should be done without infringing on the role of the states, with attention to the need to fund law enforcement to fight identity theft, and with attention to the need for private enforcement by consumers. We look forward to working with the Chair and members of the Committee, and others in Congress, to accomplish these changes for U.S. consumers. These recommendations by Consumers Union have been informed by the work of victim assistance groups, privacy advocates, and others.[11]

[11] Many law enforcers, victim assistance workers, and consumer and privacy advocates were engaged in the issue of identity theft prevention long before the most recent ChoicePoint security breach came to light. Consumers Union has worked closely for many years on efforts to fight identity theft and protect consumer financial privacy with other national groups, and with consumer privacy and anti-identity theft advocates and victim assistance groups based in California. Our views and recommendations are strongly informed by the experiences of consumers reported to us by the nonprofit Privacy Rights Clearinghouse, the nonprofit Identity Theft Resource Center, and others who work directly with identity theft victims. These groups have worked to develop the state laws that are the basis for many of the proposals now being introduced in Congress. Consumers Union is grateful for the leadership of the Privacy Rights Clearinghouse in consumer privacy policy work, the work of the state PIRGs and U.S.PIRG on consumer identity theft rights which includes the preparation of a model state identity theft statute in cooperation with Consumers Union, for the work for consumers on the accuracy of consumer credit reporting issues done over the past decade by the Consumer Federation of America and U.S. PIRG, and for the contributions to the policy debate of organizations such as the Electronic Privacy Information Center, Privacy Times, and others too numerous to mention.