AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

SUBCOMMITTEE HEARING ON DATA SECURITY: SMALL BUSINESS PERSPECTIVES

SUBCOMMITTEE ON FINANCE AND TAX
COMMITTEE ON SMALL BUSINESS
UNITED STATES HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 6, 2007

Serial Number 110-27

Printed for the use of the Committee on Small Business

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

U.S. GOVERNMENT PRINTING OFFICE

36–102 PDF WASHINGTON : 2007

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON SMALL BUSINESS

NYDIA M. VELÁZQUEZ, New York, *Chairwoman*

WILLIAM JEFFERSON, Louisiana
HEATH SHULER, North Carolina
CHARLIE GONZALEZ, Texas
RICK LARSEN, Washington
RAUL GRIJALVA, Arizona
MICHAEL MICHAUD, Maine
MELISSA BEAN, Illinois
HENRY CUELLAR, Texas
DAN LIPINSKI, Illinois
GWEN MOORE, Wisconsin
JASON ALTMIRE, Pennsylvania
BRUCE BRALEY, Iowa
YVETTE CLARKE, New York
BRAD ELLSWORTH, Indiana
HANK JOHNSON, Georgia
JOE SESTAK, Pennsylvania

STEVE CHABOT, Ohio, *Ranking Member*
ROSCOE BARTLETT, Maryland
SAM GRAVES, Missouri
TODD AKIN, Missouri
BILL SHUSTER, Pennsylvania
MARILYN MUSGRAVE, Colorado
STEVE KING, Iowa
JEFF FORTENBERRY, Nebraska
LYNN WESTMORELAND, Georgia
LOUIE GOHMERT, Texas
DEAN HELLER, Nevada
DAVID DAVIS, Tennessee
MARY FALLIN, Oklahoma
VERN BUCHANAN, Florida
JIM JORDAN, Ohio

MICHAEL DAY, *Majority Staff Director*
ADAM MINEHARDT, *Deputy Staff Director*
TIM SLATTERY, *Chief Counsel*
KEVIN FITZPATRICK, *Minority Staff Director*

SUBCOMMITTEE ON FINANCE AND TAX

MELISSA BEAN, Illinois, *Chairwoman*

RAUL GRIJALVA, Arizona
MICHAEL MICHAUD, Maine
BRAD ELLSWORTH, Indiana
HANK JOHNSON, Georgia
JOE SESTAK, Pennsylvania

DEAN HELLER, Nevada, *Ranking*
BILL SHUSTER, Pennsylvania
STEVE KING, Iowa
VERN BUCHANAN, Florida
JIM JORDAN, Ohio

CONTENTS

OPENING STATEMENTS

	Page
Bean, Hon. Melissa	1
Heller, Hon. Dean	3

WITNESSES

Milazzo, John, National Association of Federal Credit Unions	4
MacCarthy, Mark, Visa U.S.A., Inc.	6
Duncan, Mallory, National Retail Federation	8
Cochetti, Roger, CompTIA	10
DelBianco, Steve, Association for Competitive Technology	12

APPENDIX

Prepared Statements:

Bean, Hon. Melissa	28
Heller, Hon. Dean	30
Milazzo, John, National Association of Federal Credit Unions	32
MacCarthy, Mark, Visa U.S.A., Inc.	44
Duncan, Mallory, National Retail Federation	51
Cochetti, Roger, CompTIA	66
DelBianco, Steve, Association for Competitive Technology	76

SUBCOMMITTEE HEARING ON DATA SECURITY: SMALL BUSINESS PERSPECTIVES

WEDNESDAY, JUNE 6, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
SUBCOMMITTEE ON FINANCE AND TAX
Washington, DC.

The Committee met, pursuant to call, at 10:00 a.m., in Room 2360 Rayburn House Office Building, Hon. Melissa Bean [Chairwoman of the Subcommittee] presiding.

Present: Representatives Bean, Ellsworth, Heller and Jordan.

OPENING STATEMENT OF CHAIRWOMAN BEAN

ChairwomanBEAN. Good morning. I call this hearing to order to address Data Security: Small Business Perspectives. With breaches of personal data being reported with increasing regularity, the issue of data security has become one of great concern to consumers and the small businesses they do business with.

Over the past few years, tens of millions of records of data containing Social Security, bank account, credit card, and driver's license numbers have been compromised. A few weeks ago, The New York Times published a troubling cover story on identity theft in the elderly. The story discussed the data broker InfoUSA, one of the largest compilers of consumer information which sold contact lists of elderly consumers to known law breakers. The thieves posted as government officials and acquired bank account information which was used to empty out those accounts. According to the article, InfoUSA advertised lists of suffering seniors, 4.7 million people with cancer or Alzheimer's. Data brokers fall outside the scope of most current federal privacy regulations.

A major reason for the increased awareness of breaches is due to a California law implemented in 2003 that requires notice of security breaches to be sent to affected consumers. The law was the first of its kind in the nation. Subsequently, 35 states have enacted legislation requiring companies or state agencies to disclose security breaches involving personal financial information. Complying with a patchwork of state laws is challenging for all businesses and financial institutions, but particularly difficult for small firms. There have been many calls for federal legislation to address the issue of data security. In the last Congress, I introduced two data security bills and worked closely with my colleagues on the Financial Services Committee to craft a federal solution to this important issue.

As a former small business owner, I understand the value of time. Small businesses are often dependent on the efforts of few, if not one person, to run their business. Owners' regulations can take a business owner's time away from focusing on their core business and their customers. Small businesses lack in-house counsel and expertise and information security. Burdensome data security law or regulations requires small businesses to retain outside consultants and highly specialized legal and regulatory areas. Small businesses typically lack experience in managing those outside vendors and when a complicated law requires systemic changes to their IT systems, this may make them more vulnerable to expensive service agreements.

When examining this issue at the federal level, there are several considerations to keep in mind for small businesses and small financial institutions. First, a clear standard for triggering notification is critical. A vague standard could lead to a large volume of unnecessary notifications, desensitizing consumers and causing them to ignore more serious warnings. It's also important to consider that notification is costly, particularly so for small businesses to absorb.

Second, financial institutions are already subject to federal regulations on data security. Subjecting them, and small banks in particular, to a duplicate layer of federal regulations could burden them unnecessarily.

Third, while Congress should encourage adoption of best practices for securing private financial data, we should avoid mandating particular technologies in law or regulation. Security threats change rapidly and businesses must be given the flexibility to respond quickly. Firms must be able to deploy the latest security measures, mandating a particular product or technology could slow development of improved counter measures and leaves businesses one step behind the criminals.

Finally, legislation should contemplate the protection level of compromised data such as encrypted information and how much of a risk a breach realistically poses to consumers. As Congress contemplates legislation, there are steps businesses can take on their own to reduce security risks. Government may be able to play a beneficial role in education small businesses about the basics of data security.

Properly training employees can reduce the incidents of data breaches, while larger businesses with sophisticated compliance departments can create training programs, risk assessments, and written compliance plans. It's important to consider that small businesses may lack this ability and thus require assistance from regulators.

Small businesses are increasingly being confronted with the issue of data security as breaches occur with more frequency. Small firms are taking steps to better secure customer information through internal procedures and upgrading information technology. As we move forward with federal legislation on data security, unique needs of small businesses should be integral to our efforts, because compromising the profitability of small businesses would ultimately pass on costs to the very consumers we're trying to protect.

I look forward to today's testimony and thank the witnesses for their participation.

I now want to recognize Ranking Member Mr. Heller for his opening statement.

OPENING STATEMENT OF MR. HELLER

Mr.HELLER. Well, good morning, and thank you very much, Madam Chair, I know this issue is important to you and you have spent a tremendous amount of time looking into this and I appreciate your efforts. I want to also thank the witnesses that are here today, taking time out of their schedules to be in front of us today.

Nevada is one of the fastest growing states in small businesses. As Secretary of State, I was responsible for registering tens of thousands of businesses a year and I fought to keep Nevada friendly to small businesses.

I look forward to continuing to keep small business vibrant and healthy in America and in the State of Nevada. To this end, electronic commerce or e-commerce has enabled small businesses to become participants in both the national economy and the international economy. E-commerce requires data to be collected, processed, and stored electronically and transmitted across networks. Therefore, data security is a very important business requirement that requires the on-going process of exercising due care and due diligence by all participants in e-commerce. A robust national and international economy requires protecting data from unauthorized access and use.If consumers lose confidence in e-commerce based on the lack of data security, this loss of confidence will inhibit the growth ofe-commerce and small businesses, not to mention the effect of data breach can have on individual victims.

The impact on small businesses will be disproportionately greater because right or wrong, consumers will perceive large businesses offering their customers more recourse in the event of a problem. Also, all participants in e-commerce will be looking for assurances that their business partners, both large and small, are operating under proper data security policies and procedures. Any business' lack of information security readiness will spread the risk throughout all levels of the economy. What we must do is devise a way to ensure that all the parties involved are effectively protecting the information they collect without putting small businesses to a disadvantage when we do so. All too often small firms are at a distinct disadvantage when these proposals are being debated and implemented. Imposing a large one size fits all data security bill or regulation on the nation at large could be more expensive for small firms because fixed costs disproportionately impacts small businesses.

Additionally, because the owner of local hardware stores know hardware, not high-end encryption and data security services, it may require the hiring of outside vendors and consultants do implement data security and regulatory requirements because of that lack of expertise and anybody who runs a small business already knows that the time and attention of top management is already stretched too thin to be directly involved with issues such as these. Simply put, imposition of any additional costs will place small com-

panies in a competitive disadvantage because their pre-unit costs of compliance will be greater than those of large businesses.

Today, we live in a digital economy where both beneficial and potentially harmful uses of personal information are multiplying. Information about individuals is used by businesses to provide consumers with an unprecedented array of goods and services, increased productivity and protect individual businesses and society from fraud and other misdeeds.

However, that same information can also be misused to harm individuals with results such as identify theft, deception, unwarranted intrusion, embarrassment, and the loss of consumer confidence. This is a very complicated and important matter, and I applaud the Chairwoman for her leadership on this timely issue. Just yesterday, I read in the USA Today a story of how David Joe Hernandez, who returned from service overseas in the Air Force, only to find that his identity was stolen and the collection agents were hunting him down to make good on some delinquent accounts. This recent case demonstrates that all businesses must ensure consumer protection and I look forward to hearing the testimony today and working with each of you to ensure that we devise a workable plan that achieves greater security and confidence in e-commerce without harming small businesses.

Thank you, again, Madam Chairwoman. I appreciate your looking forward on this particular issue, and I yield back the balance of my time.

ChairwomanBEAN. Are there any other Members who have opening statements? Okay.

We'll now move to testimony from the witnesses. Witnesses will have five minutes to deliver their prepared statements. The timer begins when the green light is illuminated. When one minute of time remains, the light will turn yellow. The red light will come on when time is out.

Our first witness is Mr. John Milazzo. Mr. John Milazzo is president and CEO of Campus Federal Credit Union in Baton Rouge, Louisiana. He served in that role since 1985. Campus Federal is a $320 million multi-branch statewide credit union serving 39,000 members. He's testifying on behalf of the National Association of Federal Credit Unions. The membership of the National Association of Federal Credit Unions consists of the nation's innovative and dynamic federal credit unions having various and diverse membership bases and operations.

You may proceed with your testimony.

STATEMENT OF JOHN MILAZZO, CHAIRMAN, NATIONAL ASSOCIATION OF FEDERAL CREDIT UNIONS

Mr.MILAZZO. Thank you. Good morning, Chairwoman Bean, Ranking Member Heller, and Members of the Subcommittee. My name as stated is John Milazzo and I'm the present Chief Executive Officer of Campus Federal Credit Union headquartered in Baton Rouge, Louisiana. I'm testifying today on behalf of the National Association of Federal Credit Unions where I serve as the chairman of its board. NAFCU appreciates this opportunity to participate in this hearing regarding data security.

Looking to a few high profile examples, the TJX data breach has already cost Campus Federal Credit Union over $11,000. When Credit Card Systems Solution suffered a breach, Campus Federal spent over $20,000 to issue new cards and to respond to members' concerns and this does not include the detrimental effects to our institution's reputation and credibility.

In 2006, Campus Federal charged off nearly $50,000 in fraud losses on our debit cards. Additionally, Campus Federal charged off $130,000 on other fraud. The cost of insurance for credit and debit cards is increasing dramatically. In the last six years, Campus Federal's premiums have increased by more than 64 percent. At the same time, our deductible for payment card losses has also increased significantly. From 2001 to 2004, our deductible for payment card fraud and forgeries averaged $100. Today, our deductible is $1500, an increase of 1400 percent in six years.

Campus Federal's situation is not unique among credit unions. Information from those that provide bonds to credit unions indicate that credit unions incurred over $100 million in payment card fraud in each of the last few years. The costs associated with issuing a payment card can run as high as $10 or more, a cost that the 89 million Americans who are credit union members ultimately pay. Because of economies of scales, this cost is often higher for smaller credit unions.

When Campus Federal is notified a data breach impacting credit cards, we follow a 16-step flow chart that includes at least two methods of notification to our members. We also keep enough credit card stock in-house to cover at least 15 percent of our card base, allowing us to reissue cards in a very timely manner. NAFCU supports the effort to enact a comprehensive proposal to protect consumers' personal data. Credit unions and other financial institutions already protect data consistent with the provisions of the Gramm-Leach-Bliley Act. The act, and its implementing regulations have successfully limited data breaches among financial institutions. There's no similar comprehensive regulatory structure for retailers. There should be a comprehensive regulatory scheme for industries that are not already subject to oversight.

Any new legislation should create a safe harbor for financial institutions already in compliance with Gramm-Leach-Bliley. Failing to do so would place undue burden on financial institutions. AFCU believes that any data security bill should place the burden of addressing a data breach on an entity responsible for the breach. Under the current law, some industries do not have a strong enough incentive for protecting the sensitivity of their information. The first notification that people receive that their information may have been compromised is often from their credit union. Thus, the companies responsible for the data breach oftentimes do not suffer any loss of consumer good will while consumer confidence in financial institutions suffer.

Unfortunately, no matter how quickly government and industry reacts, criminals will always find a way around security measures. Therefore, it is important that there be stiff penalties to prohibit and punish the actual crooks who commit these breaches. Current data security standards with payment card companies such as Visa and Master Card prohibit storing sensitive data, yet these con-

tracts often aren't enforced and the data ends up being compromised. Some states such as Minnesota recently have enacted tougher standards to hold those responsible accountable. We believe any federal data security bill needs to do the same.

In conclusion, NAFCU believes that the most effective way to addressing the growing number of data breaches is to create a comprehensive regulatory scheme for those entities that currently have known. AFCU believes that a safe harbor for financial institutions already in compliance with Gramm-Leach-Bliley should be included in any data security bill.

Finally, financial institutions, merchants, retailers, data brokers, and any other party that holds customer information should be held financially accountable if it is responsible for a data breach. I thank you for this opportunity to appear and I would welcome your questions.

[The prepared statement of John Milazzo may be found in the Appendix on page 32.]

ChairwomanBEAN. Thank you for your testimony.

We're going to hold questions until we've heard all who are testifying today.

Next up is Mr. Mark MacCarthy who is Senior Vice President for Public Policy of Visa U.S.A. The Visa payment system is the largest consumer payment system in the world. Prior to joining Visa, Mr. MacCarthy was a principal and senior director with the Wexler Group. From 1981 to 1988 he was a professional staff member of the House Committee on Energy and Commerce.

Please proceed and thank you for being here.

STATEMENT OF MARK MACCARTHY, SENIOR VICE PRESIDENT, PUBLIC POLICY, VISA U.S.A., INC.

Mr.MACCARTHY. Thank you, Chairwoman Bean, and Ranking Member Heller and Members of the Subcommittee. I'm Senior Vice President for Public Policy as the Chairwoman Bean noted. Visa commends the Subcommittee for holding this hearing. It's an important topic, especially focusing on small businesses and I'm pleased to be able to talk about today.

Madam Chairwoman, for Visa, cardholder security is about trust. Our goal is to protect the consumers, the merchants, the banks, the credit unions and other financial institutions that are part of the Visa system by preventing fraud from taking place in the first place.

Our card security system starts with our zero liability policy which ensures that card holders are not liable for unauthorized use to their cards. And because we have that liability allocation, that creates a financial incentive for us to practice good security and to encourage our members and people associated with the Visa system to practice good security.

Because the card holders don't pay the costs of a data breach, the member financial institutions within the Visa system have to pay these costs. And as John has noted, these costs are substantial. They include the fraud losses themselves. They include the monitoring costs, the reissuance costs, the reputational risks which are intangible, but are nevertheless real. Visa aggressively protects

card holder data in order to protect our members from these financial costs.

We employ a multi-faceted approach to combat fraud. Visa has implemented a comprehensive and aggressive information security program. We call it the Cardholder Information and Security Program or CISP. This program was pioneered by Visa. It applies to all entities that store, process, or transmit Visa cardholder data including merchants, retailers and processors. And this program includes three elements. It's got the data security standards themselves. It's got compliance verification. As you're aware, companies have to demonstrate to us that they're in compliance. And there are sanctions for failure to comply with the standards.

In 2005, we issued penalties associated with failure to comply with this. It was $3.4 million in fines. In 2006, our fines went up to $4.6 million. So we're taking aggressive efforts to enforce the standards that we've got in place. This was the gold standard for data security. It's been widely imitated and thought as a model for other industries. And it's the basis for the common set of industry-wide data security requirements which is now known as the Payment Card Industry Data Security Standard.

Visa has also led the industry in providing sophisticated neural networks that flag unusual spending patterns. These neural networks enable our member banks to block a suspected transaction even before the fraud has taken place. We've also put in place a cost recovery program that enables our members to resolve disputes related to account compromises. Visa pioneered a number of other security measures designed to detect and prevent fraud. We have an Address Verification Service that matches address and other information to confirm that a transaction is valid. All of the transactions processed through the Visa system are checked against an exception file. This is the file of world-wide accounts of lost or stolen cards.

Other security measures have to do with special security codes on our cards. The Cardholder Verification Value, it's called CVV, is a three-digit code. It's included in the magnetic stripe on the card. You can't see this code on the card itself, but it's checked electronically at the time of a transaction to ensure that a valid card is present. The CVV2 code is also a special three-digit security code. It's printed on the signature stripe on the back of the Visa card. On-line or telephone merchants can verify that their customers have the actual card by requesting this security code.

For on-line transactions, we have verified by Visa which allows on-line merchants to verify that their cardholders are the people that they say they are at the time of an on-line transaction. And last, we have an Advanced Authorization Service that provides an instantaneous analysis for the potential for fraud at the very time of the transaction. As a result of these strong security measures, fraud within the Visa system is extremely low. It's about 5 to 6 cents for every $100 of transactions.

We also have a security program that's designed to address the special needs of small businesses. Small business account for the vast majority of the six million merchants that accept Visa cards in the United States. To promote sound security practices for small businesses, we've done a variety of things. We've conducted numer-

ous webinars, conference calls, and other training programs that are targeted at small merchants. We have published a number of security alerts and articles to notify banks and merchants of the latest security vulnerabilities.

In addition, Visa and the U.S. Chamber of Commerce recently conducted a 12-city nationwide data security education campaign to involve both the payments industry and merchants, including small merchants, in a fight to collect card holder information.

Madam Chairwoman, on legislation, Visa favors reasonable risk-based security and notification requirements that apply to all entities that have sensitive information. These standards should be flexible to permit an entity to consider its size and complexity as well as the nation and scope of its activities. We also believe that standards should be consistent nationwide to avoid a clash of conflicting state laws. We favor stronger penalties for identify theft and additional resources for law enforcement to combat identity theft, and we agree with John of NAFCU that the Gramm-Leach-Bliley security rules should continue to be applicable to financial institutions, but should continue to be enforced by the federal financial regulators.

Thank you for this opportunity to testify. I would be happy to answer any questions.

[The prepared statement of Mr. MacCarthy may be found in the Appendix on page 44.]

ChairwomanBEAN. Thank you for your testimony. We will come back to you with questions.

Our next testimony comes from Mr. Mallory Duncan, Senior Vice President, General Counsel for the National Retail Federation. He is responsible for coordinating strategic legislative and regulatory initiatives. NRF is the world's largest retail trade association with membership that comprises all retail formats and channels of distribution. Prior to joining NRF, Duncan served as corporate counsel in the Washington office of J.C. Penney's and was attorney advisor in the Office of Policy Planning at the Federal Trade Commission. Welcome and please proceed.

STATEMENT OF MALLORY DUNCAN, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, NATIONAL RETAIL FEDERATION

Mr.DUNCAN. Thank you, Madam Chair, Ranking Member Heller, and Members of the Committee. NRS membership includes retailers of all sizes, as you've mentioned. My focus today, however, is on our smaller members. All of us are concerned by the growth of high-tech scams that use data about individuals to commit financial fraud. Reaches have ranged from the mistaken sale of thousands of files full of sensitive personal information by brokers to criminals posing as legitimate businesses, the loss of encrypted bank account data-tapes from the cargo hold of an airplane, to criminals attacking and hacking into retailer's computer systems in order to steal card numbers.

While each of these high-profile events was disclosed to the public as a data breach, they involve a broad spectrum of nonpublic information, from the most sensitive to the least. Each poses a different level of risk to consumers and to businesses. The most sen-

sitive information, such as Social Security Numbers, driver's license numbers, and dates of birth are elements that if combined with names, addresses, and other identifying information, can lead to real cases of identity theft, that is the opening of new accounts, which a consumer is completely unaware.

These types of crimes, such as the Ranking Member just referenced, are difficult for consumers to clear up and in some cases can bring significant financial distress. They also tend to result in the greatest loss for businesses that are duped by these thieves.

The breach of other types of information, such as the misuse of card numbers, typically result in account fraud. This is the misuse of an existing account. In that case, the consumer is likely to learn of any fraudulent charges quickly, either by being alerted by their financial institutions, as Mr. MacCarthy just mentioned, or through their own monthly account review. Further, Congress generally ensure that consumers can erase bad charges or withdrawals by calling their bank or card company.

This distinction between true identify theft and card fraud is very important. Not only are the intrusions different, but the remedies that apply to one can make little sense when applied to the other. So my point number one is that data breach laws need to be carefully targeted. To date, most legislators have recognized that the public concern is not with one off thefts that result in the loss of a few files. Rather, it is the massive intentional hacks by criminals seeking tens of thousands of data files at a time that has driven this issue.

For the data thieves, this literally is a numbers game. They go where it's efficient to gather the greatest amount of useful electronic information. Fortunately, most small businesses do not store the large caches of sensitive information that can cause the most harm. Any law should be sensitive to this distinction.

Second, the proposal by some to extend data-breach notification to paper is an area of particular sensitivity for small businesses, and should be for all businesses, because of the variety of paper records required to be kept for day-to-day operations. Indeed, some are required by federal mandate.

But small businesses in particular tend to keep forms on paper. While it is conceivable that someone might steal hundreds of thousands of paper identity records, experience and common sense indicate that is not nearly as likely as a computer breach, where such a massive loss can happen at the click of a mouse. Paper breaches are more likely to be a one-off crime, and while not diminishing their impact on any single identity theft victim, they certainly do not require the same federal mandate to act as do cases involving thousands or even millions of consumers.

Fortunately, businesses and consumers have had a longer history of dealing with paper records than they have with electronic data files. Imposing a new regulatory scheme on top of existing practices would add potentially great cost for very little real benefit. Tellingly, of the 35 states that have considered and adapted data breach statutes, only two have included paper. Congress would be wise not to turn a focused bill into an unchecked regulatory burden by expanding its reach far beyond the electronic data breaches that have prompted it.

Even given that, 35 differing state laws is a lot. Frankly, a uniform national breach standard with a strong preemption is the best way to ensure that all consumers are treated fair equally when it comes to notification. Preemption would also lesson the compliance burden for all businesses and allow for one clear notice to be given to all affected customers.

Finally, and here I must disagree with my fellow panelist, Mr. Milazzo, and would be happy to go into this is in the question and answer period. Congress should proceed with caution. It is asked to allocate costs and blame in a credit card breach situation. The card associations' current system, while far from perfect for merchants and banks alike, attempts to balance the equities between all of the parties involved in a complex credit card transaction. Any interference by Congress could easily skew the cost of security for the card system disproportionately to some participants and leave issuing banks little responsibility for the ultimate security of their customers' cards.

Thank you for this opportunity to speak today and I will be happy to answer questions.

[The prepared statement of Mallory Duncan may be found in the Appendix on page 51.]

ChairwomanBEAN. Thank you, Mr. Duncan.

Our next testimony comes from Roger Cochetti, who is the group director of U.S. Public Policy for the Computing Technology Industry Association. Before coming to CompTIA, Roger was senior vice president for policy at VeriSign and a program director for policy with IBM. We welcome Mr. Cochetti's 11-year old son, Emmet, in the audience today, who I understand is attending his first congressional hearing and will be reporting back to his teacher on what he thought of it.

CompTIA has more than 22,000 member companies in over 100 countries around the world, serves as the voice of the world's 1 trillion plus IT industries, specifically all the VARS around the country and is based in Chicago, in my State of Illinois. Welcome.

STATEMENT OF ROGER COCHETTI, GROUP DIRECTOR OF U.S. PUBLIC POLICY, CompTIA

Mr.COCHETTI. Thank you very much, Madam Chair, and Ranking Member Heller, Members of the Subcommittee. My name is Roger Cochetti and I am group director of U.S. Public Policy for the Computing Technology Industry Association, CompTIA. I am here today on behalf of our 20,000 member companies. Madam Chair, I want to thank you and the Members of your Subcommittee for holding this important hearing on the state of small business data security, and I ask that my full written testimony be submitted for the hearing record.

We believe that your efforts to focus public attention on the factors that affect data security and small business will help American small business more ably address data and related IT security issues. Madam Chair, the Computer Technology Industry Association is the nation's oldest and largest trade association representing the information technology, or IT industry. While we represent every major segment of the IT industry, nearly 75 percent

of our members are small IT businesses who provide integrated computer systems to American small business.

The IT needs of American small business are mainly addressed by an important segment of the computer industry called value-added resellers, or VARs. VARs create and maintain, for example, the computer system in your dentist's office, the on-line store in which you shop on the Internet, and for your local plumber. VARs are on the front line of America's defense against IT security threats. An estimated 32,000 American VARs buy and resell about one-third of all computer hardware and software in the United States today, mostly to small businesses.

Also Madam Chair, for most people who work in the computer technology industry, CompTIA is well-known for its non-policy related services to the entire IT industry. Non-technical standards, industry education, and particularly relevant to this hearing, professional IT certifications. Some of the services that we offer that are relevant to this hearing include we have developed and managed the industry's standard basic professional certification for cyber security, which we call Security+. While almost one million American technology workers today hold some type of professional certification from CompTIA, around 35,000 hold this Security+ certification.

Over the past year, we have launched educational programs for thousands of our members on the technical implications of Gramm-Leach-Bliley and HIPAA regulations for small businesses. And in doing so have introduced the technical issues of data security to much of the small business segment. In 2005, we began a series of conferences for VARs, and through them, the small businesses that they serve on cyber security. These programs uniquely deal with small business technical issues addressing issues of IT security, cyber security, and data security.

Beginning in 2002, CompTIAs has commissioned a major annual survey on IT security. While this annual survey collects information about all sectors of the economy, about half of the participants are from small businesses, making it the countries' best barometer of small business IT security developments. The principle findings of the most recent CompTIA IT security survey are that the IT security issues of small businesses are serious and that the principal cause of IT security breaches is human error.

Among the key findings of this year's CompTIA IT security survey are nearly 34 percent of all businesses experienced an IT security breach within the last year. While that number has declined from 2005, the survey found a higher level of severity in the breaches that have occurred. Over 32 percent of all businesses reported either successful or attempted data thefts, almost double the number from 2004. And 61 percent of small businesses do not have written IT security policy in place, although a written policy without IT awareness and training doesn't amount to much.

Eighty-one percent of all participants in the survey believe that major IT security breaches can be reduced as a result of IT security training and certification. Seventy-four percent of all IT security breaches were the result of human error, either alone or in combination with a technical malfunction. Among human errors, em-

ployee failure to follow security procedures was a factor that was most often cited.

In conclusion, Madam Chair, encouraging proper IT security training and certification of all relevant employees of small businesses is the single most important step that this Subcommittee could take to promote data security among small businesses. An example of an important way to accomplish this goal is the Technology Retraining and Investment Now Act for the 21st Century, H.R. 244, which embodies principles that we have supported for some time. TRAIN would provide a federal tax credit to organizations and individuals for increasing their IT training.

More importantly, Madam Chair, is it clear to any one familiar with American small businesses that VARs much play a central role in any effort to reach out to small business in the areas of data security and cyber security. We believe that what is most needed is a government industry partnership to address small business IT security issues that takes advantage of the unique perspective of thousands of VARs in small businesses themselves. In this regard, Madam Chair, last year we called on this Committee and the Small Business Administration to create a public/private task force that would work to identify and address the IT security issues of small business.

Such a task force could include VARs, small businesses, representatives from SBA, DHS, Department of Justice, experts and providers of IT security tools. It would identify specific small business IT security issues and make recommendations. Similarly, Madam Chair, we've called on the Committee and the Department of Homeland Security and the Small Business Administration to undertake a comprehensive outreach effort on data security and cyber security specifically for small business. Using the nation's VARs as a key link in cyber security business education, we as an association and our members stand ready to cooperate with such an outreach effort. We renew both of these recommendations today.

Madam Chair, thank you again for conducting these important hearings. I'll be happy to answer any questions.

[The prepared statement of Roger Cochetti may be found in the Appendix on page 66.]

ChairwomanBEAN. Thank you for your testimony.

Final testimony is from Steve DelBianco, serving as vice president for public policy of the Association for Competitive Technology. ACT or ACT is an international grass-roots advocacy and education organization representing more than 3,000 small and mid-sized information technology firms from around the world. Before joining ACT, Steve was president of Financial Dynamics, an IT consulting firm. Thank you for being here.

STATEMENT OF STEVE DelBIANCO, VICE PRESIDENT FOR PUBLIC POLICY, ASSOCIATION FOR COMPETITIVE TECHNOLOGY

Mr.DELBIANCO. Good morning, Chairman Bean, Ranking Member Heller, Members of the Committee. I'd like to thank the chair for being a real friend to the IT and tech community and for holding hearing on the impact of data security threats and the threats of data security regulation on small businesses.

As you indicated, ACT represents thousands of tech and e-commerce businesses, many of whom handle sensitive data for customer billing and for payroll records. And as you indicated, I'm hereafter making my own small business odyssey out there in the real world. I started that IT consulting firm back in '84. Grew it to $20 million and 200 employees. And then sold it before moving to help found ACT. So I'm a small business survivor in front of you today.

Last night, I took my boys, my two boys to the Nationals game at RFK and the Nationals attempted a valiant comeback from being five runs down, only to come up one run short because the umpire completely below a call at home plate.

And my boys were very upset. They were whining about the umpire. And I stopped and reminded them, wait a minute. There's no crying in baseball. And the same is true with running a small business, I can tell you. You take what the world gives you every day. Make the best of it. You try to survive to fight the next day.

There's no crying in small business either. So I'm not here to whine. But since you asked. For the small business perspective on data security let me just share three insights and three suggestions.

Insight number one, it takes a thief to commit identify theft and card fraud. We seem to have lost sight of this some times. It's not a crime if a laptop is left at the airport or an employee walks off with my customer file. Crime happens when someone uses your card to run up charges or uses a new account in your name. So law enforcement will be a key element of any data security effort we undertake.

So insight number two, that ID theft has multiple victims. We know about the consumers, retailers, and lenders, credit unions, but there's also the business and institution who has been hacked or lost the data. Together, those victims have spent $55 billion on ID theft and card fraud in 2005, according to the Rubin & Lenard study.

And what I would like you to remember is that ten times as much of those costs were incurred by businesses, as by the consumers themselves. In other words, 50 of the 55 billion. So let's be careful not to create more victims by piling unworkable regulatory burdens on small business.

Insight number three, new costs as the chair indicated, are for security disproportionately impact small budgets. You've all heard that before, but there are those more subtle ways that small businesses are more vulnerable. An owner's attention is stretched incredibly thin and I was always too busy fighting fires to spend any time trying to prevent them. It's just the way of life of the small business. And as you indicated, it's very rare for small business to have the expertise in-house to solicit, manage, and understand what consultants are telling us when it came to complex IT issues.

This makes compliance incredibly expensive for small business. That's a lesson we've all learned with the Sarbanes-Oxley implementation which affected notably businesses that are still much larger than the small businesses affected here.

I'm not quite as convinced as my fellow panelists that we absolutely need new data protection regulation to make small business

care about data security or that new regulation would actually put a big dent in identify theft. But I'm a realist and regulation is coming. You can feel the momentum building and there's good reasons for it. Consumers, for instance, will better be able to protect themselves when they receive a notice of a data breach, provided that the notice is based on a real risk that ID theft may occur.

And second, as you heard, 35 states have now created a patchwork of notice laws and we need to replace that with the single national standard.

So if you do create a national standard data security law, I have just three suggestions from the small business perspective. Suggestion number one, we need broad and deep preemption of state laws. Gramm-Leach-Bliley preemption gives the states a floor, but no ceiling, therefore allowing the states to preserve a patchwork of state laws and even add particularly onerous state laws such as the strict liability standard that Mr. Milazzo spoke of. I believe the strict liability standard to reimburse costs incurred by banks and credit unions, even where the company that lost the data was not negligent at all in the way in which the data was lost.

The industry, the credit card industry and retailers have worked together for 20 years to build a phenomenally commerce industry through contracts in cooperation, in sharing of costs and the sharing of burdens. Legislative is not the way to interfere with an ecosystem that has worked so well for e-commerce and credit card transactions.

Suggestion number two, it's a great idea to add incentives to the business will make that maybe lost or stolen data can't be used when the bad guys get their hands on it. That is to say encryption standards. So encryption software is what most of us use today, but legislation should not lock in today's technology only. So please, make any incentives for encryption broad enough to include tomorrow's data protection technologies.

Third and final suggestion, if you're going to extend the data safeguard rules, as distinct from notice, data safeguard rules are millions of small businesses that are not currently regulated. Please don't assume that a small business will ever be able to meet the current GLB data safeguards standards. Prior data security bills in Congress, would have covered, "anyone handling personal information for interstate commerce." That is literally anyone who accepts anything other than cash for a sale. So it's true that flexibility is way better than prescriptive standards, but flexible can still be very hard and expensive for a small business. A small business really doesn't know where they are in terms of risk and they always have a tough time figuring out where they need to end up.

The PCI standards that Mark spoke of, for instance, are about 176 individual items of security compliance. That's a dizzying array for a small business to understand how to implement. Small businesses need road maps, road maps to get from where we are, to where we need to be to adhere to a standard. Regulators, I would encourage, should evaluate the best practices industries using, including PCI, a great start, and figure out where it meets the standard, and then let the eco-system of It companies, Roger's members in mind.

So in closing, just please remember that there are criminals behind ID theft and the small business is one of the victims, not the villain along with the consumers and others at the table. And please don['t force small business to implement brand new data safeguard standards until there are approved roadmaps to help small business get there.

Thank you.

[The prepared statement of Steve DelBianco may be found in the Appendix on page 76.]

ChairwomanBEAN. Thank you for your testimony.

Thank you all for your expertise and your perspective from your varying industries and from your members.

My first question is for Mr. MacCarthy. You talked about the Visa payment system and the Cardholder Information Security Program which aims to secure cardholder data, wherever that resides. I'd like to know a little bit more about how you implement that and what resources you provide to assist small businesses with complying with those standards and I want to give you an example of a couple of things I ran into just this weekend and see if they would sort of be covered in what you seek to set as your standards.

This weekend, my eighth-grader graduated and so I had a party in the back yard and called a rental company I've worked with in the past to set up a tent in the backyard and some tables and chairs and they're great to work with and they said we're all set up. I said let me give you my Visa number. They said "that's okay, I've got it right here in the system from when you did your party two years ago for your other daughter." I'm wondering if that kind of thing would be covered.

Then I took my oldest daughter, who is going to be a junior and we were going through some college brochures from College Night at the school recently. We went out to dinner to one of our favorite restaurants and when I signed my credit card, it wasn't just the four numbers on the credit card on the signature, it was the entire credit card number.

These are two local businesses that get a good amount of business. Do a great job for our community, but I'm just wondering as I saw both of those things as flags this weekend, how prevalent that is and to what degree you're seeing some of your standards curb those activities.

Mr.MACCARTHY. Let me address the two specifics first, so that we can then go on to more general enforcement for small businesses and large businesses in general. On the example of the guy getting the card and he had your information from a year before, that's a perfectly legitimate business practice. Small businesses, large businesses often have a reason to retain cardholder information. Retaining the card number for purposes of customer service, for purposes of charge backs or problems associated with the transaction later on, that's a perfectly legitimate use of the cardholder information and Visa rules do not prohibit that.

Nevertheless, if they do save that information, they are required to keep it safe and secure, but it is not a piece of information that they should be prohibited from retaining.

On the other hand, those security codes that I mentioned in my testimony, the CVV 1 and 2, those are the kinds of codes which if they're retained in a computer system and that computer system is then hacked, the person who gets that information can then go on the Internet and resell the information. That can create the possibility that a counterfeit card can be made. Without those security codes, the counterfeit card cannot be made. And so the risks of a card being manufactured and used for fraudulent transactions at a large number of other merchants is significantly lower.

So we have a rule that says do not save the security codes. There's no business reason to do that. There's no customer service involved in retaining that code. There's no verification or authorization that you need in order to save that code. Don't save the code.

So what your vendor did in that kind of circumstance as far as I can tell was perfectly legitimate in saving the number. May or may not, if he saved also the security code, that could have created a problem. We have no way of knowing that just by the description that you gave.

The truncation problem, there's a federal law, Visa was heavily involved in working with Congress with Senator Feinstein, with Members of the Financial Services Committee in putting in place a requirement in federal law that says that on the customer receipt the only thing that should appear is the last four digits of the card account number. And that's designed to create difficulty for the dumpster divers who might go in and find a receipt later on.

That's been in effect for a couple of years. There was a transition period of time to allow small businesses and others to upgrade the systems to come into compliance. That transition period has passed. And those—they should be in place already. It's the kind of thing where the FTC is beginning to look more carefully at enforcement mechanisms. There have been a number of lawsuits filed in the area to try to create more incentive for the small businesses and others to come into compliance with that. But it is a matter of federal law that you come into compliance with that truncation requirement.

More generally, we have found that the major problem in the payment card world with respect to data security comes not from small businesses, not from the six million or so small businesses that we think of as Level 4 merchants, of a small number of transactions. The major problem comes from the larger merchants. Almost the vast majority of the card accounts that are compromised come from large merchants and we have an incentive program to move them forward into compliance.

I'm happy to report that in the last several years, following the ChoicePoint incidents and the CSSI incidents, DSW and BJ's, the perception has grown among the merchant and retailer community and the processor community. That's important to practice good security.

Our compliance rates have gone up dramatically. And that key area of saving the security code, we now have among the larger merchants, 93 percent compliance and the remaining 7 percent are subject to monthly fines so we expect them to be coming into compliance with that requirement very soon.

For the more general of security rules, the whole PCI standard is such between 85 and 90 percent of our larger merchants have either given us a report that indicates that they're in compliance or have given us a report that indicates how they will come into compliance, a remediation plan for moving forward in that area. So the news is good. We still have to aggressively enforce our requirements and the intent to do so, going into the future.

ChairwomanBEAN. Thank you. I have some other questions, but I'd first like to yield to Ranking Member Heller for some questions?

Mr.HELLER. Thank you, Madam Chairwoman. I want to go to Mr. MacCarthy also. I have a Visa debit card.

Mr.MACCARTHY. Thank you. Use it well.

(Laughter.)

Mr.HELLER. It was put on hold last week during the recess.It was put on hold and I actually thank the gentleman on the other end of the line because a transaction was made in Washington, D.C., San Francisco, and Reno, Nevada in one day. And for that reason, when I went to fill up a tank of gasoline the card was rejected and we worked it out, but tell me more about that process. And what you guys do to protect the consumer under similar circumstances.

Mr.MACCARTHY. I can't speak to the exact facts of the case, but it sounds to me since you have the card, it sounds to me what happened is likely there was a data breach somewhere and the card information was improperly stored and a counterfeit card, maybe more than one counterfeit card was created based upon that stolen information. And then the fraudsters went through a number of locations and committed—

Mr.HELLER. By the way, I made all those transactions.

Mr.MACCARTHY. Pardon?

Mr.HELLER. I made all of those transactions.The transaction in Washington, San Francisco and Reno were made by me.

Mr.MACCARTHY. Okay.

Mr.HELLER. Just so you know, there wasn't misuse of the card.

Mr.MACCARTHY. I misunderstood. So the—what looked as though happened is that the neural network that I described in my testimony, looked at those pattern of transactions and said to you, that doesn't look like something you would normally do. That's out of character. It looks to us like exactly what I just described, a series of transactions that were committed by a fraudster. So to protect you and to protect themselves from the fraud losses, they put a stop on the card until they could talk to you directly and say are these transactions that you were involved in? And if you said oh yeah, I did that, then they know the problem is not a real problem. If, on the other hand you said no, no. I didn't do any of that stuff, then they know they've got a counterfeit fraud problem on their hands and they would have to re-issue the card.

Mr.HELLER. Explain again your Zero Liability policy.

Mr.MACCARTHY. That's a policy that we put in place to supplement the federal rules that exist in this area for credit cards and for debit cards. There's limitations on liability for credits cards. No more than $50 of fraudulent transactions can be charged go the cardholder. Visa and the other card companies in the last five, to six years, decided to move that policy to zero. And what it means

is that if there is fraudulent transactions on your account, if your card has been lost or stolen or it's been the subject of a counterfeit and the transactions were made, but not by you, you are not responsible for any of the losses associated with that. So in that context that I just described, if you said I didn't do that, these are not my transactions, they would immediately expunge those debts from your record and you would not be responsible for paying.

Mr.HELLER. Who is responsible for those?

Mr.MACCARTHY. As I said in my testimony, in the first instance, the entity that's responsible for those fraud losses are the financial institutions that issue you the card. So John's members would be in the first instance responsible for those fraud losses.

And that gives us a full reason to move ahead with providing good information security programs because our member banks bear the fraud loss. For example, if the card had been used at Circuit City to buy some electronic equipment, it's a fraudulent transaction. The merchant though didn't do anything wrong. So they typically get paid in that context, right? So they get their money. The cardholder is protected. He doesn't have to pay anything because it wasn't his transaction. So the entity that gets stuck paying the bill is the financial institution that issued the card, John's members.

That's why we really have to step up to do something to fix this kind of problem.

Mr.HELLER. I was wondering if the burden was more on the merchant as it was the financial institution. It is the financial institution.

Mr.MACCARTHY. Yes.

Mr.HELLER. Mr. Duncan?

Mr.DUNCAN. May I say a little bit to that? Mark is correct. The initial burden is on the financial institution. But I included in your package a charge that shows the system works. It's this. And these are the rules and regulations, Visa, Mastercard at the top of it, the issuing banks like the credit union and there are other merchant banks who actually have a contract with the individual merchants.

If it turns out in this case, now within this system, there will be reimbursement paid for cost of issuing the cards, whatever else. It was a fraud. To the credit union. But if turns out there was a breach say in—to use the example, TJX. TJX also had a merchant bank. Ultimately what happens is that the merchant bank goes back after reimbursing the credit unions and others. It goes back to TJX, outside the system and says TJX, you have to pay us. So the initial payment is made within the system so that ultimately if there's a fraud, it goes back to the retailer outside. And that's actually one of the reasons why if—this is such a complicated system. You want to be very careful before you start reallocating what's going on. We frankly think the folks in Minnesota have made a mistake because they didn't understand how this system worked when they went ahead and reallocated.

Mr.HELLER. Thank you very much. Madam Chairwoman, so you know I have a markup in a Resource Committee. I appreciate your time and energy. I want to thank all the witnesses. Congressman Jordan will take my place as we move forward.

ChairwomanBEAN. I recognize Mr. Jordan for five minutes. He has some questions.

Mr.JORDAN. Thank you, Madam Chair. What percentage of sales today are credit card versus cash or check? Any idea of the percentage?

Mr.DUNCAN. It varies with the type of merchant. Obviously, if you're talking on-line merchants, it's virtually 100 percent.

Mr.JORDAN. Right.

Mr.DUNCAN. If you're talking in a grocery store, I think the last numbers I saw were approaching 55 percent of transactions are on plastic. More traditional department stores, it might even be higher than that.

So it's the majority of purchases. Now there are other areas, for example, in fast food industry which has traditionally be a cash business where the number might be closer to 15 percent.

Mr.JORDAN. According to the Federal Reserve over half of all retail transactions are electronic inform. In the Visa system, over 60 percent of our transactions are with debit cards and over 50 percent of the dollar volume is with debit cards, not with credit cards.

Mr.JORDAN. Let me to go to, and I apologize I didn't catch everyone's testimony earlier, but Mr. DelBianco, you had mentioned in your testimony, I think this is a quote, "roadmaps not regulation" is what you would advocate. Seems to make sense to me. As much as we possibly can let the marketplace drive what has to happen on data security.

Because if a company or anybody is having some problems that's not good for business. They get an incentive to do it right. Walk me through what you mean exactly by the roadmaps versus some of the regulation that may be proposed?

Mr.DELBIANCO. Thank you, Congressman. I'll draw a distinction. The way the GLB, Gramm-Leach-Bliley data safeguards rule was implemented has turned out to create a very flexible way of addressing through an audit risk assessments and then handling. It's in the final appendix of my testimony and then various industries will then take that on. For instance, Mark's industry, the payment card industry took that on and they had currently said here's how we think banks should implement or merchants should implement GLB compliant data safeguards. And again, this has nothing to do with notification of breach. It's just the data safeguards rules that are put into place.

So what Mark considers to be a roadmap is a 12 page, 176 individual items that is very daunting as Mark will acknowledge for small businesses to implement, for small merchants to implement. So the small merchant looks at that and says there are a myriad, an infinite number of ways to actually satisfy that standard. What we need are more implementable ways to say here's a plan to implement it, if you've got a website that does e-commerce. You can very strictly say, website is doing e-commerce, capturing credit cards for single time billing. Here's the roadmap to be compliant with whatever data safeguard you issue.

So it's not just the vendor telling our small business here's what I think you ought to do and it may be compliant. The vendor would say look, here's the roadmap. This has been approved b the regulatory authority, so you can follow it. There might be a different

roadmap though. Some of my employees use laptop computers and travel with them. And there's customer data on the laptop. A different set of roadmaps for that on how I secure and encrypt that information.

And finally, let's suppose I've got some work at home moms doing tech support for me on my small tech firm and we did. Well, they're working at home on the Internet on their own computers. Well, there may be a separate set of roadmap rules for how do I secure information that shows up on their machines. These are simple implementable steps that we would welcome and actually there would be central for small businesses to be able to afford implementation.

Mr.JORDAN. Good. Thank you. Thank you, Madam Chair.

ChairwomanBEAN. Thank you. I wanted to follow up with Mr. Duncan. You talked about how the merchants are required to comply with the various standards. Can you tell me how that's working for the merchants' perspective. Are they finding it easy to comply? Is it very challenging for them? Can you give me some examples?

Mr.DUNCAN. Are you referring to the current notification standards within the states?

ChairwomanBEAN. Also from the payment card industry as well.

Mr.DUNCAN. That has been and I think Mark and I wanted to raise this, it's been challenging. This was a relatively new proposal that's come up in response to a real need, the fact that there are bad guys out there who are trying to break into systems. The difficulty for many of the larger merchants is that there is no one single way to comply. I think, in fact, there are about 221 individual requirements. And many merchants, there's some ambiguity as to some of those requirements and some of those have actually changed over time. Some of them because the payment card industry has gone back and looked at them and realized maybe we didn't say this quite right, but other times because of the face of new threats. This not bad. It's an evolving entity, but it has been extremely challenging. And of course, if your—our primary business is trying to bring product into our stores, sell merchandise, make customers happy. And if you've got all of these requirements you have to look at, as a separate part of your business just in order to be able to take payment, and if those are changing, and it's costing you millions of dollars each time you're making those changes, it can be very challenging. But we are trying very hard, as Mark said, to our largest members to get into compliance.

I think you have a very story when you're talking about smaller businesses and you have—and the payment card industry has recognized that they have to have some variation in their standards for the smaller businesses. but even there we have to be careful that we don't put on requirements that it's simply beyond the capability of a sole proprietorship to handle.

ChairwomanBEAN. Do you have perspective from the state regs as well?

Mr.DUNCAN. From the state regs, there is a fair amount of conflict out there. For example, some states may give you a great deal of flexibility to work with law enforcement before you make any notice of disclosure. Others don't give that flexibility. Well, if you've got customers coming from different states which approach do you

take and you don't want to inadvertently cross over the line. So there are real challenges which is why a uniform standard with preemption would be desirable.

Mr.MACCARTHY. Madam Chairman, can I jump in on the PCI standard issue?

ChairwomanBEAN. Yes, please.

Mr.MACCARTHY. On the question of the large merchants and their ability to comply, I think Mallory is right, this was a challenge at the beginning and there were some intense discussions before we moved ahead. The standard that Visa developed was designed for enforceability and testability. It was based upon private standard instead of being developed by ISO that were sort of general recommendations to do good things in this area.

We took that and made it specific enough so that it could actually be tested against so that an outside vendor could come in, look at a system that was designed to handle payments and say are you in compliance with these rules or not?

So it's flexible in the sense that it has many different ways of complying, but one of those ways of compliance is something that could be detected by an outside vendor and as I say in my comments before, the large merchants have moved ahead very, very effectively in this area.

The small merchants tend to be less of the problem because they have, as Mallory said, less of a honey pot for the thieves to go after. So the enforcement there has to be less stringent and our validation requirements are tiered to make sure that we don't put an unnecessary burden on the companies. Many of the small businesses, they have computer systems. And then they have the point of sale terminal that connects up to the payment system, but they don't link the two. The two are separate systems and so there's no storage of information in the computer system. When they get to be more sophisticated and they want to do more customer service, like your vendor, they might link the two systems and store cardholder information in their computer systems in a way that could create a security problem.

We have decided to move ahead with recommendations for our small businesses and for our large businesses. There are payment system applications that do not improperly store data in that context. We've listed those on our website. They're publicly available. All you have to do is go to the Visa site and find it. There's also a list of point of sale applications which we do not recommend, which have the flaw in them and we know that there is a problem associated with that. And so the small businesses and others can go there and say don't use those point of sale applications. They will create a problem.

So we're taking seriously our obligation to provide information, guidance and training for small businesses to allow them to move ahead. When they move to try to link their two systems, they can turn to Visa or to the acquiring bank that they work with for guidance on how best to do that.

Mr.COCHETTI. Madam Chair, may I offer one very quick comment and that is much of the conversation has been about the importance of procedures and this trickle down of procedures. I think it is important to keep in mind that the vast majority of instances in

which data breach occurs, particularly in small business, when it does occur, it is not a result of a failure of procedures, but it's a result of human error that occurs. You can have a merchant or small business owner or larger business owner or sort of sign up to procedures and you can have the technology tools that the vendors will provide, but if you don't have employees who are trained, and comply with them, that's where breaches very often occur. So I think the Subcommittee would be wise to keep in mind the importance of the human element in all of this. Thank you.

ChairwomanBEAN. I'd like to get back to you, Mr. Cochetti, and I also want to ask Mr. Milazzo as well, given—I know that you have entities across the country that you train with, I think you called it your Security+ Program, also have 35 state regs to try to comply with makes it difficult to have a consistent training program or to adhere to a certain best practices model, so I would think that it would serve your membership and their customers as well.

Mr.COCHETTI. Yes, I think, Madam Chair, the issue for us is probably less sensitive to the compliance questions that the retail firms and the credit card issuers have to deal with, because they're in the compliance chain. What we do in our Security+ certification is basic security tools so that one understands how they work.

For the most part, these have been able to be accommodated in the existing patchwork of state standards. However, as the patchwork itself grows and varies, it puts enormous stretches on the ability to have a standard professional certification. So you're absolutely right.

Thank you.

ChairwomanBEAN. I'd like to address that to Mr. Milazzo and for your membership, how challenging is that having 35 different laws to—

Mr.MILAZZO. It's extremely challenging. Yes, ma'am. We in the credit union industry take great lengths to train our employees as well to be compliant. We do that internally. In my instance, we have an internal training facility that actually trains any employee that has contact or have any input in the plastic card or payment system on what policies, procedures, not only are impacted by our own credit union and its policies, but those of the credit card industry itself. We take that very seriously and it's a great cost, a great burden to our institution, as I'm sure the institutions in our industry.

I might mention also that there has been a great deal of talk about small companies, or small entities and the cost of compliance. I might remind you then that in the credit union world, many credit unions are very small. Mine is a credit union of 300 and roughly $20 million in assets. In the world of financial institutions, I'm a small business. The cost, the burden to me to comply with GLB is great to me but we take it very seriously. We find a way to do that and those tools that we don't have internally, we'll find externally. We'll go to our associations or we will go to our vendors. We'll go to outside resources to make that happen.

ChairwomanBEAN. All right. I would like to open up to the panel a question that is essentially addresses what we have all been talking about on some level, in that small businesses tend to lack the

infrastructure. They don't have compliance departments, sometimes they don't have IT departments even to manage their data. What can be done to assist them, not only in the training—certainly you are doing some things, Mr. Cochetti, through your membership as far as training of employees, but in order to develop their security plans? Mr. DelBianco?

Mr.DELBIANCO. Thank you. I already sort of addressed the road map, but in a general sense, Sarbanes-Oxley would be a road map on how not to do it, a road map to nowhere. Part of it depends on the ecosystem of vendors. Roger's members and mine, who actually implement solutions for businesses that you've described, that ecosystem typically comes out of the box, handling the biggest customers first. Same with Sarbanes-Oxley. The big consulting firms took care of the largest businesses first for compliance. Those are very expensive contracts, because they're large and complex systems, but both the vendors and the customers are sort of learning the ropes as to what is going to satisfy the congressional mandate.

So it takes time—years, for those vendors to actually figure it out, come up with a cook book, their own road maps of implementing systems. They will come up with a road map for an ERP system, a road map for an in-house database. And only after they have sort of skimmed the cream of the big customers do they start to move into the middle tier and the smaller firms. So the ecosystem of industry will do a great job implementing it, but it cannot do it overnight and it will start at the top and work its way down. Therefore you need a graduated series of deadlines for implementation that are sensitive to the small businesses that will be the last ones that will be looked at. If Mark is right, that the vast majority of ID theft and card fraud occurs at very, very large institutions, I think it would be appropriate to work our way from a top down in terms of risk assessments. Thank you.

ChairwomanBEAN. Alright. Thank you. Others? Mr. Duncan?

Mr.DUNCAN. Yes, as I've suggested in my testimony, we really need to focus on where the core of the problem is first and it is the thieves who for a minimal amount of work relative to the number of names they will get will tend to focus on certain sizes and caches of data. Fortunately, small businesses aren't the prime opportunity. If there is anything that the Committee can do, the Subcommittee can do it, it would be to keep an eye out to make certain that some in a zeal to say I'm going to fix this problem once and for all, don't end up putting burdens on small businesses that are totally unrealistic. It's very important.

ChairwomanBEAN. Thank you. I think, Mr. Milazzo, you wanted—

Mr.MILAZZO. I guess I would follow by saying that I think the real cause, obviously, are all the crooks that are out there, they are looking for ways that are taking great strides in trying to find the ways to break systems. If they use those talents to do something fruitful, there is no telling what they could accomplish. I think that the real key to all of this is to keep that in mind and to put teeth into the laws that prohibit that. Those people that are found and prosecuted ought to serve time and ought to do things to make restitution to make less attractive those activities to others.

ChairwomanBEAN. Absolutely. It wouldn't be bad if we could publicize those penalties as well.

Mr.MACCARTHY. I think just to finish up, we do have small business validation dates that are significantly farther into the future than for the larger companies for exactly the reasons that they described earlier. As we get better and better at fixing the problem at the large databases retained by large processors and merchants, the crooks are going to say where else can I go? They're going to start to go down the chain and ultimately they're going to get to the smaller businesses. So we're working with the middle-sized businesses now and, you know, we're going to be ultimately having to work with the small businesses. It's a matter of time before, you know, the problem shifts down to that level. I do think we have to begin the process now so that we're ahead of the crooks. We don't wait for them to discover the new honey pots. I'm saying now we've got a rich trove here to create problems for members, for other merchants, for customers, and so on. So I think the process has to be slow. It has to be gradual, but it has to be ongoing.

ChairwomanBEAN. Absolutely. Mr. Cochetti?

Mr.COCHETTI. Just a couple. I did want to emphasize the importance that Mr. DelBianco's point earlier of differentiating among the different segments. Most of the conversation that we've had today has focused on retail merchants. Indeed, among small businesses retail merchants are important and for data security issues, perhaps the most important. But the first differentiation is the vast differentiation between large and small. But it is also important to keep in mind that among small business, almost half of the clients of our members are not retail merchants.

ChairwomanBEAN. They're B2B.

Mr.COCHETTI. Excuse me?

ChairwomanBEAN. They're B2B.

Mr.COCHETTI. Of course. Or, you know, they are attorneys, they're real estate agents, they're manicurists, they're the enormous variety. Only a quarter of the small businesses in the United States today are retail merchants. The other two thirds primarily think of themselves—they may use a credit card from time to time for billing purposes, but they don't think of themselves as retail merchants. So let's differentiate those and let's make sure that we understand that when we think about road maps, there are really very different road maps that fit very different types of small businesses. At the end of the day, the people who know this best are the merchants and the IT people who work with them because they know exactly what that business is. They know exactly what data they store and where it is stored. So I think our number one recommendation continues to be the importance of an education and outreach effort, so that the various segments can sort of among themselves begin to figure out, with help from DHS, SBA, and everyone else, can begin to figure out what makes sense for them. Thank you.

ChairwomanBEAN. I have a final question. Probably for Mr. Cochetti, but others may have some comments as well about the cost of data security insurance which has become an issue in more and more in looking at sort of cyber insurance. Some are finding it too costly. Do you have any comments on that?

For Mr. Cochetti, specifically what IT investments can small businesses make maybe as an alternative to that to better protect themselves?

Mr.COCHETTI. Madam Chair, we have found over the past few years in particular as the issues have been more visible and these liability issues have become noteworthy, that there has been the development of an insurance service for data breaches. It has been difficult for that service to reach down to small business, and I think that's one of the issues that our members have been trying to work with their customers on as sort of what can they do to develop a compliance package that would satisfy and ensure that they should qualify for coverage?

We haven't gotten there yet, but it is an on-going activity. I think on the second point, what can be done, I think the main tools that one looks to deal with this on the part of any small business are sort at the abstract level fairly common. They're procedures. They are technology tools, both hardware and principally software and then there is training. You know, I think at all three levels we work with small business to help them understand what are the best practices or what are the tools, what are the procedures that fit them. But that varies very much from segment to segment. For technology tools, there is a vast array of them available in the marketplace. There is no shortage of tools. That's the one area where you can say there is no shortage of tools available out there and training is the one that usually gets the short end of it and the one that we feel needs additional support and encouragement from the federal government.

ChairwomanBEAN. Okay, before I get to Mr. DelBianco, I just want to comment. I also in my District, we do a lot on identity theft and also Internet safety for kids. Being a parent of teenage girls, it particularly hits home for me. One of the frustrations as a parent and even as we coach people on certain things they can do, it requires a level of technical aptitude. Even though I come out of high tech, I certainly haven't been keeping up in recent years to try to protect your kids from cyber criminals.

I look to the VARs and the integrators that are out there and have said to them do any of you have a here's my, you know, kid's safe program, if I just buy that, that package, you come in, you lock everything up and now it is safe. There really isn't that. Partly because of the evolving technology, but partly because there hasn't been standards set that these are the core things you minimally have to do and different folks recommend different solutions.

So I particularly like what you're talking about here, about having a road map, trying to set some at least core best practices to try to achieve in the industry.

I know, Mr. DelBianco, you wanted to add some comments of your own?

Mr.DELBIANCO. Thank you, Madam Chair. Appendix A to my testimony included a simple chart which I called the security stack. It's really just meant to imply that there is no silver bullet, no one point of vulnerability, but a whole stack. Of course, it starts with user habits and human error and goes all the way down to networking and support.

ChairwomanBEAN. Physical error, yes.

Mr.DELBIANCO. Exactly. But the one place where because you asked the question of where would you start, and one place you would start is the second layer of the stack called the application software. That would take care of the problem that Mark MacCarthy brought up. First thing that business would do is to encrypt customer account numbers. If they have to store them at all, you encrypt them so that if a breach should occur through some other layer of the stack, the data itself is not subject to abuse. That allows the risk trigger to be pulled and the company doesn't have to do notice. The company doesn't have to go through the problems, because it's not going to create a risk of identity fraud.

ChairwomanBEAN. Thank you.

Mr.COCHETTI. Just if I could briefly say that many of the tools that have been developed for industry are applicable to consumers in home use. But there's a very substantial effort under way which I am happy to say CompTIA is a supporter and founder, to develop tools and services for consumers at the home level to provide on-line safety for children.

Mr.MACCARTHY. Madame Chairman, can I jump in on the—

ChairwomanBEAN. I'm going to let you, you know, each make a comment on this because we're going to wrap on this one. I think we've covered—no, I did ask Mr. Jordan. He didn't have a question. So go ahead, Mr. Duncan.

Mr.DUNCAN. I think your question illuminates something. It's very important for small businesses. They are running a business, and while IT may be part of that business, they frankly don't know—

ChairwomanBEAN. They don't want to be in that business.

Mr.DUNCAN. They don't know a lot about what is going on. We had a case of a retailer who had a cash register system within his store, and he frankly thought he was fully compliant, that he was not preserving the kinds of codes, and he knew enough to ask the vendor that if information is going being stored, and he was told not.

Well, what happened of course was that the information was being stored, but it was wiped out at the close of each business day. So from the vendor's standpoint, the information was not being stored.

ChairwomanBEAN. Not being stored.

Mr.DUNCAN. And from the retailer's standpoint, he thought he had done—he knows no more about what's in that system than I know what is going on in my Windows. And yet, he found himself subject of a data breach because someone, a former employee of that company realized that there was a back door and was pulling the data out at 4:30 in the evening before he shut down. So we have to be realistic about what is actually achievable, and not put knowledge burdens on merchants that they literally can't achieve.

ChairwomanBEAN. Well, it's your point many parents—talked about parents wanting to just buy safety for their children. Small businesses want to buy—just give me the Security+ package. I don't want to have to learn it or know it. I'm focused on revenue generation, I don't want to have focus on that. So I think that to the degree that we can achieve a roadmap where there will be

those in the business who can offer that as a commodified product in the market.

Mr.DUNCAN. And just finally, because it's a very competitive business and profit margins are very thin, you can't buy that system here.

ChairwomanBEAN. Well, every business model is different to the degree to how much you're storing and how much customer or financial information you're keeping as well.

Mr.MILAZZO. Madame Chair, I think your original question had to do with insurance. I might want to share with you the fact that in the financial industry, and particularly in credit unions, we find that the cost as I had shared with you earlier is going up. It's increasing from year to year with the coverage for plastic card and payment card systems. It's gotten to the point too that many of the insurers have found that not to be a profitable business—

ChairwomanBEAN. Thank you, Emmet.

(Laughter.)

ChairwomanBEAN. That is not a profitable business in spite of the rise in the premiums, to the point that some are actually considering, as I understand, dropping that coverage. If they do that, it gives financial institutions fewer choices to go to for that type of insurance which only drives that cost up from those that do provide it. It may cause some financial institutions to self-insure, which is I think somewhat dangerous. Or, in other cases, to sell their portfolios, which means basically they get out of the business. I think all those are detrimental.

ChairwomanBEAN. All right, Mark, did you have a final comment, too?

Mr.MACCARTHY. A comment on Duncan's example of the retailer doesn't know what—I mean, that's one reason why Visa took the step of putting the approved payment applications on the Internet and putting the disapproved one on there at all. Maybe the retailer shouldn't know that, but the vendor who is providing the service would be able to check the site and get one of the application programs that doesn't save it even for a brief period of time. So we're trying to do what we can to get the information out into the marketplace to resolve exactly those kinds of difficulties.

On Steve's mention that, you know, the first thing to do is encrypt the data—maybe. One of our requirements is protect, store data. It is not encrypt, store data. There may be reasons why in a given kind of circumstance that encryption isn't the right solution. You might have to redact it or otherwise make it unusable. So the requirement is protect the stored data, which actually has an implication for legislation. We shouldn't have something that says encrypt and only encrypt. The standard in the legislation should be encrypt the information or otherwise make it unusable. It's the kind of standard that is already built into what the industry is doing.

ChairwomanBEAN. Well, thank you all for your insightful testimony. In conclusion, I'm going to ask unanimous consent that members will have five days to submit statements and supporting materials for the record. No one is here to object, so without objection, so ordered this hearing is now adjourned.

[Whereupon, at 11:31 a.m., the hearing was concluded.]

STATEMENT
Of the Honorable Melissa Bean, Chairwoman
United States House of Representatives, Committee on Small Business
Subcommittee on Finance and Tax
Full Committee Hearing: "Data Security: Small Business Perspectives"
Wednesday, June 6, 2007, 10:00 a.m.

I call this hearing to order to address "Data Security: Small Business Perspectives."

With breaches of personal data being reported with increasing regularity, the issue of data security has become one of great concern to consumers and the small businesses they do business with. Over the past few years, tens of millions of records of data containing Social Security, bank account, credit card, and driver's license numbers have been compromised.

A few weeks ago, *The New York Times* published a troubling cover story on identity theft and the elderly. The story discussed the data broker infoUSA, one of the largest compilers of consumer information, which sold contact lists of elderly consumers to known lawbreakers. The thieves posed as government officials and acquired bank account information which was used to empty out accounts. According to the article, infoUSA advertised lists of "Suffering Seniors," 4.7 million people with cancer or Alzheimer's disease. Data brokers fall outside the scope of most current federal privacy regulations.

A major reason for the increased awareness of breaches is due to a California law, implemented in 2003, that requires notice of security breaches to be sent to affected consumers. The law was the first of its kind in the nation. Since then, 35 states have enacted legislation requiring companies or state agencies to disclose security breaches involving personal information. Complying with a patchwork of state laws is challenging for all businesses and financial institutions, but it is particularly difficult for small firms.

There have been many calls for federal legislation to address the issue of data security. In the last Congress I introduced two data security related bills and worked closely with my colleagues on the Financial Services Committee to craft a federal solution to this important issue.

As a former small business owner, I understand the value of time. Small businesses are often dependent on the efforts of few, if not one person, to run the business. Onerous regulations can take a business owner's time away from focusing on their core business. Small businesses lack in house counsel and expertise in information security. Burdensome data security law or regulations require small businesses to retain outside consultants in highly specialized legal and regulatory areas. Small businesses typically lack experience in managing outside vendors. When a complicated law requires systematic changes to their IT systems, this may make them more vulnerable to expensive service agreements.

When examining this issue at the federal level, there are several considerations to keep in mind for small businesses and small financial institutions:

Firstly, a clear standard for triggering notification is critical. A vague standard could lead to a large volume of unnecessary notifications, desensitizing consumers and causing them to ignore more serious warnings. It is also important to consider that notification is costly, and particularly for small businesses to absorb.

Secondly, financial institutions are already subject to federal regulations on data security. Subjecting them—and small banks in particular—to a duplicative layer of federal regulations could burden them unnecessarily.

Thirdly, while Congress should encourage adoption of best practices for securing private financial data, we should avoid mandating particular technologies in law or regulation. Security threats change rapidly, and businesses must be given the flexibility to respond quickly. Firms must be able to deploy the latest security measures. Mandating a particular product or technology may slow development of improved countermeasures and leave business one step behind criminals.

Finally, legislation should contemplate the protection level of compromised data, such as encrypted information, and how much of a risk a breach realistically poses to consumers.

As Congress contemplates legislation, there are steps businesses can take on their own to reduce security risks. Government may be able to play a beneficial role in educating small businesses about the basics of data security.

Properly training employees can reduce the incidence of data breaches. While larger businesses with sophisticated compliance departments can create training programs, risk assessments, and written compliance plans, it is important to consider that small businesses may lack this ability and thus require assistance from regulators.

Small businesses are increasingly being confronted with the issue of data security. As breaches occur with more frequency, small firms are taking steps to better secure customer information through internal procedures and upgrading information technology. As we move forward with federal legislation on data security, the unique needs of small businesses should be integral to our efforts, because compromising the profitability of small businesses will ultimately pass on costs to the very consumers we are trying to protect.

I look forward to today's testimony and thank the witnesses for their participation.

Opening Statement
June 6, 2006
Subcommittee on Finance and Tax
Data Security: Small Business Perspectives
Rep. Dean Heller, Ranking Member

Good morning and thank you Madame Chair for holding this hearing. I would also like to extend my thanks to our witnesses who have taken time out of their schedules to provide this subcommittee with testimony today.

Nevada is one of the fastest growing states for small businesses. As Secretary of State, I was responsible for registering thousands of businesses a year and I fought to keep Nevada friendly to small businesses. I look forward to continuing to keep small businesses vibrant and healthy in America and the state of Nevada.

To this end, Electronic commerce, or "E-Commerce," has enabled small businesses to become participants in both the national economy and the international economy. E-Commerce requires data to be collected, processed and stored electronically and transmitted across networks. Therefore, data security is a very important business requirement that requires the ongoing process of exercising due care and due diligence by all participants in E-Commerce.

A robust national and international economy requires protecting data from unauthorized access and use. If consumers lose confidence in E-Commerce based on the lack of data security, this loss of confidence will inhibit the growth of E-Commerce and small businesses—not to mention the effect a data breach can have on individual victims. The impact on small businesses will be disproportionately greater because, rightly or wrongly, consumers will perceive large business' offering their customers more recourse in the event of a problem. Also, all participants in E-Commerce will be looking for assurances that their business partners, both large and small, are operating under proper data security policies and procedures. Any business' lack of information security readiness will spread the risk through all levels of the economy.

What we must do is devise a way to ensure that all of the parties involved are effectively protecting the information they collect without putting small businesses at a disadvantage when we do so. All too often, small firms are at a distinct disadvantage when these proposals are being debated and implemented. Imposing a large one size fits all data security bill or regulation on the nation at large could be more expensive for small firms because fixed costs disproportionately impact small businesses.

Additionally, because the owner of the local hardware store knows hardware, not high-end encryption and data security services, it may require the hiring of outside vendors and consultants to implement data security and regulatory requirements because of that lack of expertise--and anybody who has run a small business already knows that the time and attention of top management is already stretched to thin to be directly involved with issues such as theses. Simply put, imposition of any additional costs will place small companies in a competitive disadvantage because their per-unit cost of compliance will be greater than those for large business.

Today we live in a digital economy where both beneficial and potentially harmful uses of personal information are multiplying. Information about individuals is used by businesses to provide consumers with an unprecedented array of goods and services, increase productivity, and protect individuals, businesses and society from fraud and other misdeeds. However, that same information can also be misused to harm individuals, with results such as identity theft, deception, unwarranted intrusion, embarrassment, and loss of consumer confidence.

This is a very complicated and important matter and I applaud the Chairwoman for her leadership on this timely issue. Just yesterday I read in USA Today a story of how David Joe Hernandez, who returned from service overseas in the Air Force, only to find that his identity was stolen and that collection agents were hunting him down for make good on some 20 delinquent accounts. This resent case demonstrates that all business must ensure consumer protection and I look forward to hearing the testimony today and working with each of you to ensure we devise a workable plan that achieves greater security and confidence in E-Commerce without harming small businesses.

I yield back the balance of my time.

Testimony of

John Milazzo

President/CEO of Campus Federal Credit Union

On behalf of
The National Association of Federal Credit Unions

"Data Security: Small Business Perspectives"

Before the
House Small Business Committee
Subcommittee on Finance and Tax
United States House of Representatives

June 6, 2007

National Association of Federal Credit Unions
3138 10th St. North
Arlington, VA 22201
(703) 522-4770
www.nafcu.org

Introduction

The National Association of Federal Credit Unions (NAFCU) is the only national organization exclusively representing the interests of the nation's federally chartered credit unions. NAFCU is comprised of over 800 federal credit unions—member owned financial institutions across the nation—representing more than 27 million individual credit union members. NAFCU–member credit unions collectively account for approximately two-thirds of the assets of all federal credit unions. NAFCU and the entire credit union community appreciate the opportunity to participate in this hearing regarding data security.

Historically, credit unions have served a unique function in the delivery of necessary financial services to Americans. Established by an act of Congress in 1934, the federal credit union system was created and has been recognized as a way to promote thrift and to make financial services available to all Americans, many of whom would otherwise have no access to financial services. Congress established credit unions as an alternative to banks and to fill a precise public need—a niche that credit unions continue to fill today for over 89 million Americans. Every credit union is a cooperative institution organized "for the purpose of promoting thrift among its members and creating a source of credit for provident or productive purposes." (12 USC 1752(1)). While over 70 years have passed since the *Federal Credit Union Act* (FCUA) was signed into law, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

- Credit unions remain totally committed to providing their members with efficient, low cost personal service; and,
- Credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

Credit unions are not banks. The nation's 8,305 federally insured credit unions serve a different purpose and have a fundamentally different structure, existing solely for the purpose of providing financial services to their members. As owners of cooperative financial institutions united by a common bond, all credit union members have an equal say in the operation of their credit union—"one member, one vote"—regardless of the dollar amount they have on account. These singular rights extend all the way from making basic operating decisions to electing the board of directors—something unheard of among for-profit, stock-owned banks. Unlike their counterparts at banks and thrifts, federal credit union directors generally serve without remuneration—a fact epitomizing the true "volunteer spirit" permeating the credit union community.

Credit unions have an unparalleled safety and soundness record. Unlike banks and thrifts, credit unions have never cost the American taxpayer a single dime. While the Federal Deposit Insurance Corporation (FDIC) and the Federal Savings and Loans Insurance Corporation (FSLIC) were both started with seed money from the United States Treasury, every dollar that has ever gone into the National Credit Union Share Insurance Fund (NCUSIF) has come from the credit unions it insures. Furthermore,

unlike the thrift insurance fund that unfortunately cost hundreds of billions of dollars, credit unions have never needed a federal bailout.

I am currently the President and CEO of Campus Federal Credit Union, headquartered in Baton Rouge, Louisiana. I am testifying today on behalf of the National Association of Federal Credit Unions, where I serve as the Chairman of its Board of Directors. Campus FCU Union has $332 million in assets and more than 37,000 members. Campus FCU is one of the oldest credit unions in the United States. It was formed in 1934 by ten employees of Louisiana State University and was issued charter number 79.

I have nearly forty years of experience in the financial services industry, having worked for several Louisiana banks before joining Campus Federal Credit Union as President and CEO in 1985. I have also served on the Federal Reserve Bank of Atlanta's Financial Institutions Advisory Committee. Additionally, I am the past Chair of the Southern Financial Exchange, a regional automated clearinghouse association. I also serve as a member of the Advisory Board for XP Systems, a leading computer software developer. In 2005, I was appointed to the Fannie Mae National Advisory Council. Finally, I currently serve as the Chair of the Finance Committee of Saint Anne's Catholic Church.

The Data Security Problem

As the members of this subcommittee well know, data breaches are a significant problem for both consumers and businesses. The number and breadth of data breaches are so great that it is difficult to calculate losses incurred to both the consumer and financial institution as a result of compromised data with any sort of specificity. The Federal Trade Commission (FTC) estimates the cost to be in the millions of dollars each year for new account losses when circumstances such as a criminal opening up a credit card account in a victim's name occur. While a comprehensive figure is difficult to determine, I can tell you that data breaches have cost Campus FCU and our member owners a significant amount of money.

Looking to a few high profile examples, the TJX data breach has already cost Campus FCU over $11,000. When Credit Card Systems Solutions suffered a breach, Campus FCU spent over $20,000 total to issue new cards and respond to our members' concerns, and this does not include the credibility and reputation issues that are discussed below.

In 2006, Campus charged off just under $50,000 in fraud losses on our debit cards. Additionally, Campus charged off over $130,000 in other fraud stemming from forgery, skimmed account numbers and stolen cards. Additionally, the cost of insurance for credit and debit cards is increasing dramatically. In the last six years Campus' premiums for payment card fraud coverage have increased by more than 64 percent. At

the same time, Campus' deductible for payment (credit & debit) card losses has also increased significantly. From 2001 to 2004, our deductible for payment card fraud and forgeries averaged $100. Today, our deductible is $1,500, an increase of 1,400 percent over six years.

Campus FCU's situation is not unique among the credit union community or the financial services industry as a whole. Analysis has shown that credit unions incurred over $100 million in payment card fraud in each of the last two years. Although it varies by institution, the cost associated with reissuing ATM and debit cards can run as high as ten dollars or more, costs that the 89 million Americans who are credit union members ultimately pay.

Dealing with potential data security issues is an issue that many credit unions are spending more and more time on in recent years. For example, when Campus is notified of a data breach impacting credit cards, we follow a 16-step flow chart, that includes at least 2 methods of notification to our members. We also keep enough credit card stock in house to cover at least 15% of our credit card base, allowing us to reissue cards in a very timely manner.

In addition to the cost credit unions and other financial institutions incur in notifying consumers, issuing new cards, changing account numbers, etc., there is also considerable cost, both in money and time, for consumers. Those that must have their cards re-issued may face the inconvenience of losing access to their credit or debit cards

for a period of time. If that member were a small business who needed to use those cards on a daily basis, their business could be impacted as well. Furthermore, although an individual whose identity has been stolen many not necessarily incur large out of pocket expenses, they may find the process of repairing identity theft and restoring credit a very time consuming ordeal.

There can be added costs in the form of credit monitoring services for those who are dedicated to ensuring they do restore their credit and don't become repeat victims. The victim may also request several credit reports each year from the three major credit reporting agencies in order to ensure that there is no unauthorized activity taking place in their name. When a credit union member is a victim of identity theft, the credit union oftentimes will work with them and help them monitor their credit union account.

Protecting Consumer Information

NAFCU supports efforts to enact a comprehensive proposal to protect consumers' personal data. Credit unions and other financial institutions already protect data consistent with the provisions of the Gramm-Leach-Bliley Act (GLB). There is no comprehensive regulatory structure similar to GLB for retailers, merchants or others who collect or hold sensitive personal information. While NAFCU supports new measures to combat data breaches, any new legislation should create a safe harbor for financial institutions already in compliance with GLB; failing to do so would place an undue burden and cost on financial institutions that would be forced to retool systems that they already have in place.

Consistent with Section 501 of GLB, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards (1) to ensure the security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require that third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

GLB and its implementing regulations have successfully limited data breaches among financial institutions. The best way to move forward and address data breaches is to create a comprehensive regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. By and large, financial institutions have not been the source of significant data breaches. It would be redundant at best and possibly counter-productive to authorize any agency - other than the functional financial institution regulators - to promulgate new, and possibly duplicate or contradictory, data security regulations for financial institutions already in compliance with GLB.

Accountability for Those Who Do Not Protect Consumer Information

The burden of addressing a data breach should fall on the entity responsible for the breach. Under the current law, some institutions and industries do not have a strong enough incentive for protecting sensitive information, as evidenced by the widespread number of data breaches that have been reported over the last several years.

There are two motivating factors as to why those who collect and hold sensitive information do not do enough to protect it. First, the cost associated with the data breach often falls on others. Second, because others – for example a financial institution issuing the payment cards with new numbers – generally have to repair the problems caused by a data breach, consumers often incorrectly assume that these institutions were responsible for the breach. The first notification that they get that their information may be compromised is often a call or letter from their credit union. By looking out and taking care of their members, credit unions (and other financial institutions) can unintentionally suffer some ill will from a member who finds out that their payment card from that institution has been re-issued. Thus the companies responsible for the data breach in the first place oftentimes do not suffer any loss of customer goodwill, at the same time consumer confidence in financial institutions, such as credit unions, may suffer.

While, the reputation risk to financial institutions may be difficult to solve with legislation, Congress should consider holding accountable those companies that are responsible for significant data breaches. Obviously, data breaches are going to continue

to be a fact of life for any company that holds personal information. Unfortunately, no matter how quickly government and industry reacts, criminals will always find new and inventive ways around security measures. Even with everything that financial institutions and other parties can do to protect data, it is important that there be stiff penalties and full enforcement of the laws that prohibit and punish the actual crooks who take the action to commit these breaches by stealing, and often selling or using this compromised data.

Nonetheless, any data security bill should place the burden of addressing a data breach on the entity responsible for the breach, whether it is the financial institution, retailer, data broker, or any other third party. The entity at fault that did not adequately protect the data in accordance with best practices and the law should be responsible for all direct costs associated with loss, including notifying regulators, law enforcement and credit bureaus, while covering the costs incurred by financial institutions in their efforts to protect consumers who have been affected by the security breach. It is not our intent to have data breaches put any company out of business. Instead, we believe that there must be a strong incentive for businesses to properly protect consumer's financial data, otherwise, as evidenced by recent instances of payment card breaches, the information may not be adequately protected and the credit union could end up being the one that pays.

It is with this in mind that NAFCU believes it is important that any bill approved by Congress include language to reimburse, in a timely manner, impacted financial institutions for the direct cost that they incur due to a data security breach that was no

fault of their own. While some may believe that interchange fees are designed to address this issue, the true intent of interchange fees was to meet the costs of the credit processing system (including limited fraud) and not to cover the impact of major breaches and the costs associated with the failure to adequately protect data. Without additional federal incentive to comply and protect data, any legislation that does not increase the burden on responsible parties could end up being a paper tiger. Current data security standards with payment card companies such as Visa and Mastercard prohibit storing sensitive data and even impose fines for those that do, yet, either because the penalties are not harsh enough or the contracts aren't enforced, data ends up being stored and breaches still end up happening. Some states, such as Minnesota recently, have enacted tougher standards to hold those responsible accountable. We believe any federal data security bill needs to do the same.

Finally, it should be noted that financial losses to credit unions are especially troubling, because unlike banks and other financial institutions, credit unions do not make profits for shareholders, do not issue stock and aren't able to turn to capital markets for money to make up for data breach losses. All monies at a credit union must be raised through their members. Financial losses to the credit union are ultimately passed back to the member in the form of either reduced services, lower dividends on savings, higher interest rates on loans (either personal or business), or even decreased availability of loans.

As mentioned above, financial institutions often suffer the loss of goodwill as consumers often think their credit union or bank is responsible for the breach because they must re-issue plastic, change account numbers, etc. However, financial institutions are rarely the source of a data breach. Merchants, data brokers and others, however, have been shown to have kept records of their customers' financial account information without adequately protecting it. As such, NAFCU supports placing the financial burden for repairing the damages associated with a data breach on the entity responsible.

Conclusion

NAFCU supports new measures to ensure industry takes adequate steps to protect consumers' sensitive financial data. The most efficient way to address the growing number of data breaches is to create a comprehensive regulatory scheme for those entities that currently have none. NAFCU believes that a safe harbor for financial institutions already in compliance with section 501 (b) of Title V of the *Gramm-Leach- Bliley Act* (GLBA) should be included in any data security bill. Further, if more regulations are needed to address new concerns, it should be the functional regulators that are charged with promulgating new rules. Finally, merchants, retailers, data brokers or any other party that holds customer information should be held financially accountable if it is responsible for a data breach.

STATEMENT

OF

MARK M. MACCARTHY

ON BEHALF OF

VISA U.S.A. INC.

BEFORE THE

SUBCOMMITTEE ON

FINANCE AND TAX

OF THE

COMMITTEE ON SMALL BUSINESS

UNITED STATES HOUSE OF REPRESENTATIVES

Data Security: Small Business Perspectives

June 6, 2007

Chairwoman Bean and Members of the Subcommittee, my name is Mark MacCarthy. I am the Senior Vice President for Public Policy for Visa U.S.A. Inc. ("Visa"). Visa appreciates the opportunity to address the important issues raised by today's hearing on data security and small businesses.

The Visa Payment System, of which Visa U.S.A. is a part, is a leading consumer payment system, and plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud.

Visa commends the Subcommittee for focusing on the important issue of data security and its impact on small businesses. As the leading consumer e-commerce payment system in the world, Visa considers it a top priority to remain a leader in the development of technology, products and services that protect consumers from the effects of information security breaches. As a result, Visa has long recognized the importance of strict internal procedures to protect the customer information of our members.

Visa has substantial incentives to maintain and promote strong security measures to protect customer information. Cardholder security is never just an afterthought in the transaction cycle at Visa. For Visa, it's about trust. Our goal is to protect consumers, merchants and our members from fraud by preventing fraud from occurring in the first place. This commitment to fighting fraud extends to Visa's Zero Liability policy, which protects Visa cardholders from any liability for fraudulent purchases. Because the financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholder customers, these institutions incur costs from fraudulent transactions. These costs primarily are in the form of direct dollar losses from credit that

will not be repaid. They also include card replacement costs, fraud monitoring costs and incremental customer service costs. In order to protect our members from these costs, Visa aggressively protects their customer information.

Visa's Information Security Programs

Visa employs a multi-faceted approach to combat account fraud and identity theft. Visa has implemented a comprehensive and aggressive customer information security program known as the Cardholder Information Security Program ("CISP"). This security program applies to all entities, including merchants, that store, process, transmit or hold Visa cardholder data, and covers entities that operate through brick-and-mortar stores, mail and telephone order centers and the Internet. CISP was developed to ensure that the customer information of Visa's members is kept protected and confidential. CISP not only includes data security standards, but also provisions for monitoring compliance with CISP and sanctions for failure to comply.

In addition, Visa has successfully integrated CISP into the common set of data security requirements used by various credit card organizations without diluting the substantive measures for information security already developed in CISP. Visa supports this common set of data security requirements, which is known as the Payment Card Industry Data Security Standard ("PCI Standard"). To help accelerate compliance with the PCI Standard and to eliminate the storage of sensitive card data, Visa launched the Visa PCI Compliance Acceleration Program to provide acquirers with financial incentives for their merchants' validation of compliance and to expand monetary fines for the storage of prohibited data and noncompliance with the PCI Standard.

Visa also provides sophisticated neural networks that flag unusual spending patterns for fraud that enable our members to block the authorization of transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institutions and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of cards, Visa again notifies the issuing institutions, which begin a process of investigating and evaluating the need to reissue cards.

Similarly, Visa has implemented a new Account Data Compromise Recovery ("ADCR") process to resolve disputes related to account compromises that have been linked to magnetic strip-read counterfeit fraud. The ADCR process is used exclusively when magnetic strip data is determined to be compromised. Once a merchant notifies its acquirer of an account compromise, the acquirer sends the stolen card account numbers directly to Visa's Compromised Account Management System. Visa then validates that an account compromise has occurred and notifies issuers about the compromised accounts. Affected issuers can monitor or close the compromised accounts or block transactions that are attempted on such accounts.

Visa has implemented a number of other security measures designed to detect and prevent particular fraudulent transactions:

- Visa's Address Verification Service matches shipping and billing addresses and other information to confirm that a transaction is valid.
- Visa maintains an exception file comprised of a worldwide database of account numbers of lost or stolen cards and other cards that issuers have designated for confiscation or other special handling. All transactions

processed through the Visa system have the account numbers checked against this exception file.

- The Cardholder Verification Value ("CVV") is a unique three-digit code included in the magnetic strip located on the back of all Visa cards. The CVV is electronically checked during the authorization process for card-present transactions to ensure that a valid card is present.
- The CVV2 is a unique three-digit code printed on the signature strip on the back of all Visa cards. These codes help merchants confirm that cardholders are in possession of the actual card. Online merchants or telephone merchants conducting transactions when the card is not present can verify that their customers have the actual card by requesting the customer to provide the CVV2 number.
- Verified by Visa both protects customers and allows merchants, including all kinds of small businesses, to avoid charge-back costs in online transactions by having cardholders authenticate their identities while shopping online. Its password protection reduces the potential for fraud over the Internet.
- Advance Authorization provides an instantaneous analysis of the potential for fraud at the time of a transaction.

As a result of these strong security measures, fraud conducted within the Visa system ranges from five to six cents for every $100 of transactions.

Visa also has security programs that focus specifically on small businesses, which account for the vast majority of the more than 6 million merchants that accept Visa cards in the U.S. To promote sound security practices for small merchants, Visa has:

- Conducted numerous webinars, conference calls and other training programs targeted at small merchants.
- Developed the Payment Application Best Practices to promote the use of secure payment applications that do not cause the storage of sensitive data.
- Distributed a list of vulnerable payment applications that have been found to cause the storage of sensitive data.
- Published a number of security alerts and articles to promptly notify acquirers and merchants of the latest security vulnerabilities.

In addition, Visa and the U.S. Chamber of Commerce recently conducted a 12-city nationwide data security education campaign to involve both the payments industry and merchants in the fight to protect cardholder information and reduce fraud. Visa believes that all parties that participate in the payment system, including small businesses, share responsibility to protect cardholder information.

Pending Data Security Legislation

Visa has not taken a position on specific data security legislation that is pending. In general, we favor reasonable risk-based security and notification requirements that would apply to all entities that have sensitive customer information. However, these standards should take into consideration the size and complexity of an entity's business, as well as the nature and scope of its business activities. As noted above, Visa believes

that all participants in the payment system, including small businesses, share responsibility to protect cardholder information. Nonetheless, most small businesses often do not engage in practices, such as storing credit card transaction data, that create incentives for thieves to attack their systems. Visa's validation requirements recognize this fact by adopting a tiered approach that allows small businesses to self certify their compliance with the PCI Standard.

We also believe that security and notification standards should be consistently applied nationwide to avoid a clash of conflicting state laws in this area. Finally, we favor stronger penalties for identity theft and additional resources for state and local law enforcement to combat identity theft.

Thank you, again, for the opportunity to present this testimony today. I would be happy to answer any questions.

STATEMENT OF THE

NATIONAL RETAIL FEDERATION

SUBCOMMITTEE ON FINANCE AND TAX
HOUSE COMMITTEE ON SMALL BUSINESS

"DATA SECURITY: SMALL BUSINESS PERSPECTIVES"

WEDNESDAY, JUNE 6, 2007

Liberty Place
325 7th Street NW, Suite 1100
Washington, DC 20004
800.NRF.HOW2 (800.673.4692)
202.783.7971 fax 202.737.2849
www.nrf.com

Good morning, I am Mallory Duncan, Senior Vice President and General Counsel for the National Retail Federation. I appreciate the opportunity to testify at today's hearing. By way of background, the National Retail Federation is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet, independent stores, chain restaurants, drug stores and grocery stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.6 million U.S. retail establishments, more than 24 million employees - about one in five American workers - and 2006 sales of $4.7 trillion. As the industry umbrella group, NRF also represents more than 100 state, national and international retail associations. NRF's membership consists of retailers of all sizes from single store sole proprietorships to publicly-owned retailers with hundreds of thousands of employees. Regardless of size, retailers and our customers are concerned by the growth in increasingly sophisticated high tech scams that use individuals' data to commit financial fraud. We need to look at all of the tools available to help us effectively fight these crimes. Our focus in this hearing today is the issues confronting NRF's smaller member companies.

Surprising increases in the reported number of identity thefts and instances of credit card fraud led to a significant amount of testimony before Congress in 2002 and 2003, as part of a series of hearings held on the reauthorization of the Fair Credit Reporting Act. Indeed, Congress went on to establish many new protections for identity theft victims in the Fair and Accurate Credit Transactions Act (FACTA),

including the right to block fraudulent information on their credit reports and the creation of new fraud alert systems so that new credit would not be extended to identity thieves. After extensive rulemaking, many of these new rules and protections are now just coming on-line, and we still have much work left to do.

As many members of the Subcommittee may be aware, a few months before the FACT Act was signed into law, a new California statute was enacted requiring the public disclosure of electronic security breaches under certain circumstances. This law, and the subsequent data breaches that it has caused to be made public, have brought the issues of data security, consumer privacy and identity theft to the forefront like never before, unfortunately eclipsing the very important work Congress did to protect consumers just two and a half years ago. These breaches have ranged from the mistaken sale of thousands of files full of sensitive personal information to criminals posing as legitimate businesses, as in the case of Choice Point, to encrypted data tapes containing account information literally disappearing in the cargo hold of a plane, as in the case of Bank of America. In the retail sector, reported cases have involved criminals attacking and hacking into retailers' computer systems in order to steal customer credit card information.[1]

While each of these high-profile events was disclosed to the public as a "data breach," they involve a broad spectrum of consumer information, from the most sensitive to the least, and each poses a different level of risk to consumers. The most sensitive information, including a consumer's SSN, driver's license number or date of birth are elements that, if combined with a name and address, can lead to real

[1] While the press often reports "brand-name" retail or financial institutions involved in data breaches, they often do not report similar instances in the public sector or at colleges and universities, who, according to the Privacy Rights Clearing House, are the most common sources of data compromises.

cases of identity theft – that is the opening of new accounts in a consumer's name that the consumer has no knowledge or control over. Often these types of crimes are difficult for the consumer to clear up and, in some cases, can bring significant financial distress.

The breach of other types of information, such as a credit card or account number, likely can only result in account fraud – the misuse of a consumer's *existing* account. In this case, the consumer is likely to know of any fraudulent charges very quickly either by being alerted by their financial institution or through their own monthly account review. Further, victims can easily erase any bad charges or withdrawals through a simple call to their bank or credit card company. In many cases, if the bank catches the unauthorized charges first, they are simply removed from the customer's account. Congress enacted these protections as part of the Truth in Lending Act (TILA) and the Fair Credit Billing Act (FCBA) and the Electronic Funds Transfer Act (EFTA). This distinction between true identity theft and credit card account fraud is very important. Not only are the intrusions different, but the remedies that apply to one make little sense in the other context.

To date, most state and federal legislators have shown great sensitivity to the need to target those areas of greatest concern rather than adopting broad, overly-inclusive laws. Thus, for example, the state laws regarding data breach notification have overwhelmingly recognized that the public concern is not with one-off instances of data theft that have resulted in the loss of a few files. Rather, it is losses such as the massive, intentional hacks by criminals seeking thousands of data files at a time that has the been the biggest concern. For the data thieves this literally is a numbers

game. They go where it is efficient to gather the greatest amount of useful electronic information. Fortunately, most small businesses do not generally store these large caches of sensitive information that the thieves most value.

There is currently no federal law that governs all uses of information about consumers. Perhaps the most notable federal financial privacy statute is Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA). It requires financial institutions to safeguard the security and confidentiality of customer information. A "financial institution," as defined under GLBA, holds much more sensitive information about a consumer than just that customer's credit card account number; it holds all of the information needed to complete the opening of an account and for conducting a continuing relationship with that customer. On the other hand, most retailers and other small businesses only retain the most basic credit card account information for the purposes of completing a single transaction in which merchandise or services are given in consideration for payment by the customer.

We believe it would be an unfair regulatory burden for Congress to require onerous new security standards similar to those found in GLBA to be applicable to the entire business community. This would be particularly burdensome for small businesses which, if found in violation of such mandated standards, could be subject to a law enforcement action by the Federal Trade Commission. Small businesses and retailers of all sizes would be at a further disadvantage in this scenario because financial institutions are regularly subject to examination by regulators and often aided and advised in their compliance efforts. As you know, the FTC, as a law

enforcement agency, is unable to provide this type of assistance, and non-compliance by a covered entity would likely result in stiff fines.

Instead, we hope that if Congress acts in this area, that they give measured consideration to how it would affect businesses of all types and sizes. The need for such a national standard, if any, should vary according to economic sector, business model, and business size. This cannot be a "one size fits all" type of mandate, and education assistance by agencies such as the Small Business Administration would be critical in aiding small businesses in their compliance efforts. As you may be aware the Federal Trade Commission just launched a program aimed at educating small businesses about information security practices.

The extension of data breach notification to paper is an area of particular sensitivity for small businesses, and should be for all businesses, because of the amount of paper records that are required to be kept in the day-to-day operation of business, including by federal mandates. But small businesses, in particular, tend to keep forms on paper. While it is conceivable that someone might steal hundreds of thousands or even millions of paper identity records, experience and commonsense indicate that is not nearly as likely as a computer breach where such a massive loss can happen at the click of a mouse. Paper breaches are more likely to be a "one-off" crime, and while not diminishing their impact on any single identity theft victim, they certainly do not require the same mandate to act as in cases involving thousands or even millions of consumers

Because of the nature of paper records, versus their electronic cousins, it is often hard to determine if paper documents have been breached and which records

have actually been compromised. Would a business actually know if a dishonest employee has broken into the HR office after hours and taken a handful of his colleagues' prior year W-2 tax forms? Would any company be able to tell with any certainty which customers' information was compromised if a file of documents were misplaced or vanished? These complications only scratch the surface and for Congress to treat paper and electronic breaches the same would over-simplify the unique set of challenges for businesses who store, process and dispose of paper on a regular basis.

Fortunately, businesses and consumers have had a much longer history of dealing with paper records than they have with electronic data files. The steps that businesses reasonably take, such as keeping employment records in locked file cabinets have kept the risks inherent in this type of fraud to a manageable level. Imposing a new regulatory scheme on top of existing practices would add potentially great costs for very little real benefit. Tellingly, of the 35 states that have considered and adopted data breach statutes, only two, North Carolina and Hawaii, have included paper. Congress would be wise not to turn a focused bill into an unchecked regulatory burden by expanding its reach far beyond electronic data. We would ask that the members of this Committee be particularly sensitive to the burdens such an extension of the proposed data breach laws would have on modest sized businesses.

Finally, as set forth in the Appendix to this testimony, there is an issue not directly related to the Congressional role in this matter, inasmuch as it involves contracts among the financial institution parties in the current credit card system, that

nevertheless has been much discussed of late. We include this material to demonstrate the complexity involved in dealing with just one segment of this issue.

Conclusion

As Congress moves to consider data security legislation again this year, it is important to point out elements that will be most beneficial to small businesses and their customers. First, a uniform national data breach standard with strong preemption is the only way to insure that all consumers are treated equally when it comes to notification. Preemption would also lessen the compliance burden for all businesses and allow for one clear notice to be given to all effected customers. Current state laws are generally written to cover residents of that state, not businesses that conduct business there. This means that under the current patchwork of state laws even small businesses could conceivably run into a multi-state compliance burden just by having customers from another state make purchases in their store, whether in person or over the internet.

Members of Congress should also take into consideration the fact that for most businesses the most sensitive piece of customer information they possess is a credit card number. Retailers, for instance, typically do not have other sensitive information such as Social Security Numbers. Further, a data breach resulting in the loss of a credit card number may at worst lead to credit card fraud, which is easily detected and resolved, and not the more insidious crime of identity theft. As a result, legislation should treat the breach of account information differently that the breach of more sensitive data.

Congress should also forbear from including paper in the type of breach notification legislation that was originally designed by the states to cover only electronic data breaches. These very different types of information media require completely different security solutions, and we believe that one-size fits all legislation would be a mistake.

Finally Congress should proceed with caution while trying to allocate costs and blame in a breach situation. The card associations' current system, while far from perfect for merchants and banks alike, attempts to balance the equities between *all* of the parties involved in a complex credit card transaction. Any interference by Congress could easily skew the cost of security for the credit card system disproportionately to merchants and leave issuing banks little responsibility for the ultimate security of their customers' cards.

APPENDIX

As the Committee may appreciate, there has been a great deal of media attention focused on large computerized thefts of data. The retail industry as seen its share. But because the media often does not understand the distinction between true identity theft and credit card fraud, both the serious and less serious breaches get lumped together in stories under the more serious identity theft moniker, clouding the public discourse on this issue. As was mentioned, this is very troubling because these crimes are very different, and warrant different responses from victims, businesses and the credit-granting industry, which in turn may warrant different responses by Congress.

Regrettably, in recent months some have attempted to use the unfortunate hack attack on TJX to vilify merchants and the standard of care given by retailers to credit card data. This has led to confusion and misinformation about what a retailer's responsibilities are vis-à-vis the banks and credit card associations for both providing security for credit card transactions in their stores and allocating the costs associated with a breach event. First, I must state emphatically that merchants of all sizes take the security of their business information, including account number information, seriously. Card-accepting merchants of all sizes are attempting to adopt private security procedures that have been rolled out jointly by the major credit card brands over the past few years: the Payment Card Industry security standards ("PCI").

The card industry is extending versions of these requirements to all merchants who accept credit cards – including small retailers, restaurants, charities, doctor's offices, veterinary clinics, travel agents, government agencies, hotels, airlines, schools, universities, beauty salons and spas to name a few

While a worthwhile effort, PCI has unfortunately consisted of ever shifting requirements, entailing huge investments in time and cost . These changes have left many affected businesses faced with the prospect of repeatedly modifying their programs to meet less than clear card association requirements. Many businesses have dealt with the added challenge of modifying legacy computer systems or dealing with vendors who themselves may not be PCI compliant. This is especially troubling for small retailers who purchase their cash registers and software packages "off the shelf," and rely on manufacturers' representations that the equipment is, in fact, PCI compliant. Nevertheless, NRF is assisting our members efforts to adapt to these procedures.

To add to the confusion about card security, there seems to be a general misunderstanding as to what type of data merchants are permitted to retain under the PCI guidelines. Subsequent to authorization retailers are, in fact, allowed to keep account numbers, cardholders' names and expiration dates in their systems. This is done for many business-worthy reasons including processing payments, merchandise returns, and as proof of the transaction in the event of a dispute or retrieval request. Without this information merchants would be hard-pressed to meet their obligations both to the issuing banks and to consumers. It is the most sensitive data, such as service codes, CVV/CVV2, and card association-reserved values that

must be removed once the initial transaction is complete. Further, a merchant is not permitted to keep the *full* contents of certain track data from cards' magnetic stripes.

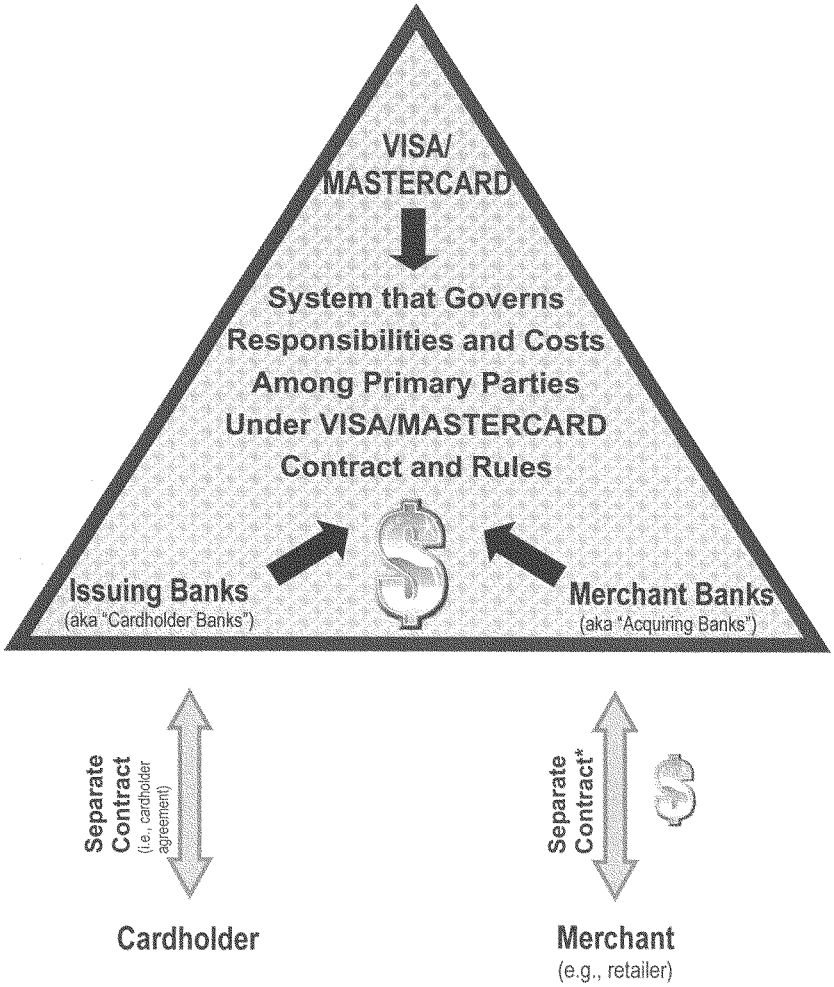
In event of a breach, there is a streamlined procedure in place at the card associations in which the effected accounts are reported. Visa calls its system "CAMS," or the Compromised Account Management System. Under this system, Visa investigates the breach and then sends a CAMS e-mail alert to the affected issuers to notify them of potentially compromised accounts. Often, it is a false alarm. The affected issuers then monitor, close or block their credit card accounts. In the case of larger banks, credit cards are generally monitored for fraud, and accounts are only closed if the incidence or rate of fraud indicates that this is a necessary step, i.e. the alarm was genuine. However, many small or medium sized community banks or credit unions, much to the dismay of merchants, do not monitor for fraud under the current system but instead cancel and re-issue cards en masse.

As with every aspect of the contractual agreement between a merchant and the credit card associations, the issue of who pays in event of a breach event is set forth in the contract signed by all of the parties. Under Visa and MasterCard's rules, the breached retailer's acquiring bank is liable for the incremental fraud costs during the event window (typically 12-13 months). Further, issuing banks participating in the process can also recoup money to cover operating expenses such as card re-issuance and increased customer service calls. The charges incurred by the acquiring bank are then passed back to the merchant or breached entity.

Recently, some state legislatures have begun looking at the reimbursement process, in particular due to complaints by small banks and credit unions that they

are not being reimbursed at the highest desired rate.[2] However, because of the complex contractual obligations between a retailer, the retailer's acquiring bank, the card associations and the consumer's issuing bank, we urge Congress to carefully consider any quick legislative "fixes" in any data breach legislation moving forward. The card associations' current system, while far from perfect for merchants and banks alike, attempts to balance the equities between *all* of the parties involved in a complex credit card transaction. Any interference by Congress should be very measured as it may skew the cost of security for the entire credit system disproportionately to merchants and leave small issuing banks little responsibility for the ultimate security of their customers' cards. Any legislation requiring retailers to pay for data breach costs could be particularly devastating for small merchants, who are already the victims of a criminal attack when data theft occurs, and who are already likely to pay stiff fines to the card associations and acquiring banks.

- [2] The dollar amounts that the small banks are claiming for reissuing a credit card are very high in comparison to larger institutions. We have seen their estimates as high as $35. In truth, it should only cost a few dollars to reissue a credit card.



* Typically contract between merchant bank and its retailers requires retailers to reimburse merchant bank for any costs, penalties, or fees imposed by the system on the merchant bank (including chargebacks – i.e., disputed charges – and costs of data breaches)

PAPER

Finally, Congress should carefully consider any regulatory regime that casts a wide net over many different types and sizes of business. While we believe that all businesses should be under the general obligation to secure sensitive information, from HR records to credit card information, one size may not fit all. Currently, the FTC is actively asserting its jurisdiction under the FTC Act to go after businesses whose lapses in data security have risen to the level of unfair and deceptive trade practices. Businesses of all size are on notice that data security is a serious issue and continued education can go a long way to help prevent future breaches.

Unfortunately, no matter what Congress does, the crooks will always be one step ahead of the latest security systems, and it is important to recognize that in many cases these businesses, big and small, are being victimized by sophisticated white-collar criminals.

Testimony of

The Computing Technology Industry Association (CompTIA)

Roger J. Cochetti

Group Director-U.S. Public Policy

Before the House Small Business Committee

Subcommittee on Finance and Tax

On

"Data Security: Small Business Perspectives"
Wednesday, June 6, 2007

Good morning, Chairwoman Bean, Ranking Member Heller, and distinguished members of the Subcommittee. My name is Roger Cochetti. I am Group Director for U.S. Public Policy of the Computing Technology Industry Association (CompTIA) and I am here today on behalf of our 20,000 member companies.

Madam Chairwoman, I want to thank you and the Members of your Subcommittee for holding this important hearing on the state of small business data security. Data security breaches, often caused by opportunistic cyber criminals and frequently enabled by human errors, can be prevented by, in most cases, using the right combination of training, technology tools, procedures, and public/private sector collaboration. We believe that your efforts to focus public attention on the factors that affect data security and small business will help American small businesses more ably address, thwart and remediate data security threats.

CompTIA: Association Overview and Role in IT Security.

The Computing Technology Industry Association represents the business interests of the information (IT) industry. For 25 years, CompTIA has provided research, networking and partnering opportunities to its 20,000, mostly-American, member companies. While we represent nearly every major computer hardware manufacturer and software publisher, nearly 75% of our membership is comprised of American Value Added Resellers, or VARs. These small, system integrators set up and maintain computer systems and networks for small businesses. An estimated 32,000 American VARs sell some $43 billion dollars worth of computer hardware, software and services -- mostly to the small businesses that drive the American economy. This means that around one-third of the computer hardware and software sold in the U.S. today is sold by VARs; again mostly to small businesses. VARs are the front line in protecting critical data from cyber criminals. We particularly appreciate the opportunity to testify before this Subcommittee, because for our VAR members, data security is not a theoretical concern: It is what they must build into the services that they provide to their clients.

As this Subcommittee knows, small business is the backbone of the American economy. Some 23 million small businesses employ over half of the private sector workforce and are a vital source of the entrepreneurship, creativity and innovation that keeps our economy globally competitive. They are responsible for over half of our GDP, and their share is growing. Moreover, Americans depend upon small business for virtually every aspect of their daily lives. So, as a nation, we are dependent upon the health of the small business sector. And small business, in turn, relies on our members for its information technology services.

VARs service just about every small business in America. Your dentist, travel agent, local retailer, or dry cleaner almost certainly contracts with their local VAR to install, maintain and service their IT needs. For example, the local area network in your dentist's office is most likely not installed or maintained by the dentist. Nor is it installed and

maintained by a multinational computer hardware or software company. This work is almost certainly performed by a local VAR.

While CompTIA is distinct in its representation of Americas tens of thousands of VARs, I wish to also emphasize that we represent most of America's principal computer hardware, software, and services companies. In addition to representing the interests of our members through our headquarters in Chicago, and our public policy offices in Washington, Brussels, Hong Kong and Sao Paulo, CompTIA works to provide global policy leadership for the IT industry, and nowhere are we more active than in the area of cyber security policy.

Finally Madam Chairwoman, for most people who work with computer technology, CompTIA is probably best known for the non-policy-related services that it provides to advance industry growth: standards, professional certifications, industry education and business solutions.

In order to most efficiently serve the industry and our members, CompTIA has developed specialized initiatives and programs dedicated to major areas within the IT industry. Some of the services that we offer that are relevant to this hearing include:

· Professional Certifications for IT Workers

CompTIA offers 12, vendor-neutral professional certifications that test and validate a variety of baseline technical and professional IT skills. CompTIA A+, Network+, CDIA+, PDI+, Server+, Linux+, IT Project+, Convergence+, CTT+, DHTI+ (Home Technology Integrator), RFID+, and Security+ certifications provide credibility, recognition of achievement and quality assurance for employers and employees alike.

Today, almost one million CompTIA certificates have been issued; mostly to American IT professionals. And these CompTIA 'alumni' are an important source of insight and input for us as we address issues like data security and cyber security.

Importantly for this hearing, we have developed the Security+ professional certification. Security+ is the industry standard for validating an IT professional's abilities in the areas critical to data security including infrastructure security, communications security, operational security, and basic cryptography. For the business community, Security+ certified employees and contractors means a reduced risk of network breaches and an improved ability to prevent and mitigate cyber crime. To date, around 35,000 people have taken our Security+ certification exam, making it the most important cyber security professional certification in the United States.

· Helping the IT Industry Understand Privacy Regulations

CompTIA provides a formal structure and method for managers in the IT industry to communicate and resolve industry issues such as standard terminology in warranties and how to address new and challenging regulations that IT companies collectively face. We have launched a series of parallel efforts to help the industry understand the complexities, and implications for IT integrators, of such recent Federal regulations in the area of consumer privacy as those resulting from Graham-Leach-Bliley (GLB) and the Health Insurance Portability and Accountability Act (HIPAA). Threats to consumer privacy under the practices regulated by these laws and regulations very often result from cyber crime. This is as true for small businesses as it is for large companies.

· Educating VARs and Other Small IT Companies on Cyber Crime

With support from Federal and State officials and many of our larger member companies, in 2005 we launched a series of modest educational outreach programs for VARs on the problems and issues raised by cyber security. These new programs aim to reach out to the thousands of small IT businesses that make up the bulk of our membership and help them better understand what the Federal and State governments and large corporations are doing in this area and explain how they can get more involved.

· Public Policy

CompTIA's public policy program addresses the policy and regulatory concerns of the IT community at the federal, state and international levels. We do this by educating our members about developments in the policy process and encouraging them to get more engaged and by advocating policy solutions that make sense for the nation and for the IT industry.

Given the importance of small business to the U.S. economy and the importance of VARs as the IT enablers of small business, it is somewhat surprising and disappointing to us that cyber crime and data security concerns of small businesses have not received greater attention. At the federal level, several important but modest efforts have been launched aimed at educating small business about the basic issues in IT security; and we are pleased to say that we have been involved in nearly all of them. As I will explain later, we believe that much more needs to be done, however.

The State of Small Business IT Security.

Beginning in 2002, CompTIA has commissioned an annual IT security benchmark study entitled "Committing to Security – A CompTIA Analysis of IT Security and the Workforce." This study is a cross-sector analysis of the state of IT security as well as an examination of the root cause of most IT security breaches.

The benchmark study surveys professionals across a myriad of industries who are asked to answer pressing questions about the dynamic landscape of IT security. Our study also provides insights into IT security practices and highlights security challenges confronted by organizations of varying sizes and sectors. Approximately 28% of the respondents are small businesses with annual revenues below $10 million, and another 20% are businesses with annual revenues from $10 million to less than $100 million.

To briefly summarize, CompTIA's IT Security Study reveals that the IT security landscape has changed significantly, along with the rapidly changing technology used across industries. As we all know, the opportunities of Internet communications and commerce in the global marketplace have been exploited by some with malicious intent. Although procedures and cyber security technology tools have become increasingly more advanced in their ability to detect security threats to networks, applications and operating systems, malicious hackers are often sophisticated enough to find gaps in procedures, failures to comply with procedures, or to reverse-engineer technology tools. Even the most sophisticated cyber security procedures or technology tools, however, cannot replace the need for IT security training and certification in the workplace.

Most non-technology based organizations are slower to adopt new procedures, cyber security tools and slower to implement cyber security training and certification for employees. Employees with cyber security responsibilities, but without adequate training and certification, can easily underestimate a threat of security breaches to their organization. Other decision-makers, including small business managers, lack the empirical support to rationalize the needed investment for IT security.

Overall, CompTIA's Cyber Security Study reveals a large discrepancy between the IT security that organizations say they need and the level of education and prevention occurring within these organizations. In 2006, the fifth annual CompTIA Study on IT Security and the Workforce found that nearly 34% of organizations experienced an IT security breach within the last year. While that number has declined from 2005, the survey found a higher level of severity in the breaches that did occur. On a scale of 1 to 10, with 10 being most severe, the average breach in 2005 was a 2.3; in 2006 that number grew to a 4.8.

More specifically, while the study found that over 32% of respondents reported facing data theft issues, up dramatically from 19.8% in 2004, and 50% of respondents reported that data theft threats had increased over the past year, it also found that organizations, including small businesses, may not be taking all the steps necessary to protect

themselves. 61% of small businesses do not have a written IT security policy in place, and small businesses are less likely to report a security breach.

Overwhelmingly, 81% of responding organizations believe that major security breaches have been reduced as a result of IT security training and certification. The positive effect of training and certification is most often described in terms of improved potential risk identification, increased awareness, improved security measures and an ability to respond more rapidly to problems. The lack of written IT security policies for more than 60% of the responding small businesses fosters gaps in security knowledge, especially among end-users. Even in organizations with written security policies in place, enforcement of security policies continues to be a problem.

Combating Data Security Breaches: Training and Technology Used to Fight Cyber Criminals and Prevent Human Errors.

Madam Charwoman, we have found that data security breaches at businesses generally occur as a result of one or more of the following: Low-tech crime; high-tech (or cyber) crime, and human error. Low tech crimes are represented by more traditional criminal activity, such as physically stealing a computer from an office, home or car, or a company's employee stealing information or hardware from the workplace. VARs use technology tools such as password protection and encryption to help prevent criminal access to data if it has been stolen using low-tech methods, and can use low-tech physical tools, such as computer locks and lockers, to prevent physical theft. Obviously, CompTIA's members do not commonly address the physical security concerns that are the first line of defense against low-tech crime. But we are quite concerned with the physical aspects of IT security and most of our members work with their customers to improve basic physical computer security.

Cyber crime, as distinct from low-tech crime, often does not involve the physical removal of computer hardware from a business. A cyber criminal doesn't need to physically go

inside a business to steal data. Criminals can remotely enter computers and steal data using malicious software programs distributed via email, email attachments and internet downloads. Additionally, data could be accessed by cyber criminals entering a business' wireless network using a laptop in the vicinity of the business. Our members help their customers by using procedures and technology tools both to prevent malicious programs from entering a businesses network and to prevent unauthorized entry into the network. For procedures and technology to be effective, both the technology integrator and the end user need to thoroughly understand the procedures and the technology tools themselves. To that end, our members can also provide basic employee training for a customer's employees on how to identify and prevent security breaches, and can use their own training to mitigate the damage caused by such a breach.

While having security procedures and having security tools installed are critically important to preventing data security breaks, human error is by far the single most important cause of preventable cyber security breaches. Not following, understanding or bypassing security technology and protocols is the real world equivalent of leaving a businesses back door unlocked or neglecting to turn on the alarm system. According to CompTIA's IT Security Survey, human error, either alone or in combination with a technical malfunction, was blamed for three out of every four IT security breaches (approximately 74%). Security assurance continues to depend on human actions and knowledge as much, if not more so, than it does on technological advances. More than half the organizations surveyed (55.5%) reported the failure of staff to follow security procedures as the factor that contributed to most breaches caused by human error. Encouraging the proper training and certification of all relevant employees, in particular employees of small businesses, we believe is the single most important step this Subcommittee could take to protect the data controlled by small businesses.

Recommendations & Conclusion.

Based on our studies and the real world experiences of our members and certification holders, it is very clear that more needs to be done to raise IT security education, training and certification within the U.S. small business community. This segment of the American economy is almost entirely dependent for its IT enablement on VARs -- of which there are tens of thousands across the country. These VARs hold the key to reach small business, helping them improve their data security awareness and preparation. Small businesses and VARs alike, however, are struggling to find trained and certified employees, which our survey reveals is the most critical element in preventing IT security breaches.

To that end, one of the most important things Congress can do to improve IT security and prevent data breaches is to increase the pool of trained and certified IT employees. An important way to accomplish that is to enact the Technology Retraining and Investment Now Act for the 21st Century (TRAIN Act—H.R. 244), an idea we have supported federally and at the state level for the better part of a decade. The TRAIN bill will provide a tax credit for 50% of information and communications technology training program expenses. Just as the research and development tax credit helps companies make continuous investments in new product development, today a complementary human resources technology development tax credit is necessary to assure that there is a trained workforce capable of combating IT security breaches.

It is also clear to anyone familiar with small businesses in the United States that VARs must play the central role in any effort to reach out to small business in the areas of cyber security and data security. What is most needed is a government industry partnership that takes advantage of the unique access and perspective of the thousands of VARs who IT-enable small business in the U.S.

In this regard, Madam Chairwoman, last year we called on this Committee and on the Small Business Administration to create a public-private task force that would work to

identity IT security issues of small businesses. We believe it is important to focus on small businesses as a sector, as some issues are more unique to small businesses, while other issues might be less germane. This task force could include representation from SBA and DHS, would identify specific small business cyber security issues and make recommendations for resolution of such issues. Whatever the specific charge of this task force, we believe it is most important that we lay the groundwork now to maintain the security and productivity of existing small businesses, and those yet to be established.

Similarly, we have called on the Committee, the Department of Homeland Security, and the SBA to launch an aggressive education and outreach effort on data security and cyber security aimed specifically at small businesses using this nation's VARs as the key link in cyber security small business education.

We renew both of those recommendations today, Madam Chairwoman, and hope this Subcommittee will act on them.

In conclusion, I would like to again thank the Subcommittee for holding such an important hearing, and I, along with our 20,000 members, look forward to working with this Subcommittee to prevent data security breaches at small businesses.

Statement of Steve DelBianco

Vice President for Public Policy,

The Association for Competitive Technology (ACT)

Testimony before the

House Committee on Small Business,

Subcommittee on Finance and Tax

Hearing on

"*Data Security: Small Business Perspectives*"

June 6, 2007

Chairwoman Bean, Ranking Member Heller, and distinguished members of the Committee: My name is Steve DelBianco, and I am Vice President for Public Policy for the Association for Competitive Technology (ACT). I would like to thank the Committee for holding this important hearing and I'm pleased to have the opportunity to testify on the impact of data security threats—and the threats of data security regulations—on small business.

ACT is an education and advocacy group for small, technology-based businesses. We represent over 3,000 small tech firms and e-commerce businesses, including many that accept credit card payments and handle sensitive customer data for testing or hosting customer billing and payroll applications.

ACT advocates for a "Healthy Tech Environment" that promotes innovation, competition and investment. Two indicators of a healthy tech environment are a high degree of consumer trust & confidence, and low regulatory burdens for businesses. Both these indicators are under attack from criminals who steal business information in order to pursue credit card fraud and identity theft.

I also come before you having made my own small business odyssey: In 1984 I founded an IT consulting firm, and grew it to $20 million in sales and 200 employees over 13 years, then sold the business to a national firm before helping to start ACT.

Data Protection is an important issue for small business, especially e-commerce retailers. Data protection legislation from the prior and current Congress would require consumer notification of a breach, and would require the implementation of security measures to safeguard consumer information. Notification and data security are distinct subjects and each matter could merit its own Congressional hearing. While several House bills combine the two issues, for purposes of this hearing and my testimony, it is helpful to separate notification from data protection when analyzing the regulatory impact on small businesses.

Why Data Security Regulation is So Expensive for Small Business

What's unique about the perspective of small business in assessing the impact of data protection regulation? The first two answers to this question are widely known:

- Fixed costs disproportionately impact small business, and this is equally true of costs for data protection measures required by regulation. The Securities Exchange Commission has reacted to widespread complaints that smaller businesses were chafing at the million-dollar cost of implementing financial reporting systems to comply with Sarbanes Oxley regulations.
- Small business is rarely at the table when laws and regulations are being crafted. This is not to suggest that lawmakers and agencies fail to consider the interests of small business. Indeed, the Regulatory Flexibility Act requires special analysis for proposed rules that "*would have a substantial economic impact on a substantial number of small entities.*"[1] And when the FTC was preparing data safeguard rules pursuant to the Gramm-Leach-Bliley Act (GLB) back in 2002, it sought comments on the costs to small entities, but reported that "*no commenters provided specific cost information.*"[2] Our government frequently asks for input, but it's not surprising that small business owners rarely scan the Federal Register or find the time to respond with specific cost information.

In addition, there are less obvious aspects to why small business is particularly vulnerable to new threats and new regulatory requirements:

- In a small business, the time and attention of top management is stretched thin. The top of the management pyramid in a small business is narrow (often just the owner), so their time is consumed by cash management and crisis management. To put it simply, a small business owner is usually too busy fighting fires to pay much mind to preventing new ones – even when they know they should.
- It's exceedingly rare for a small business to have in-house legal counsel or in-house expertise in the products and practices of information security. Nor do small businesses have a "bench" of talented executives to which they can delegate special projects, such as an initiative to improve data protection and regulatory compliance.

---

[1] Federal Register / Vol. 67, No. 100, May 23, 2002, Rules and Regulations by the Federal Trade Commission, regarding 16 CFR Part 314, "Standards for Safeguarding Customer Information; Final Rule", p. 36491.

[2] Ibid, p. 36491.

During the GLB rulemaking, a few trade associations told the FTC that small businesses would be disproportionately burdened "*because they lack expertise (relative to larger entities) in developing, implementing, and maintaining the required safeguards*"[3].

- Moreover, small businesses don't have the expertise to solicit, select, and manage outside vendors and consultants in areas that require specialization and experience. This "asymmetry of expertise" tends to make small business more susceptible to expensive implementation contracts and service agreements, especially when data security vendors are encouraged to mitigate risks by over-engineering their proposed solutions.

[3] Ibid, p. 36491.

THE CRIME AND COSTS OF IDENTITY THEFT

There are multiple victims in any consumer data breach. Consumers are the most obvious victims, but so too are the businesses that suffered the breach, particularly small business. When criminals breach customer data held by a small business, they place at risk the very survival of that company. It's essential to remember that although data can be lost many ways, "It takes a thief" to make data loss into a crime.

"It Takes a Thief" to Commit Identity Theft

With all of the press accounts, statistics, and assorted approaches to legislation, it seems we've lost sight of the root cause that's driving demand for data protection regulation. If a data tape falls off a delivery truck, or a sales rep loses her laptop computer, no crime has yet been committed. It takes a thief to turn these losses into crimes, by charging someone else's credit card or opening new credit accounts in their name.

Imagine a new series in the popular *CSI* genre: ***CSI: Identity Theft:***

> The premier episode features a criminal gang called ShadowCrew, who's made a science out of identity fraud. They've got 4,000 gang members operating around the world using the latest technology to coordinate, communicate, and trade in stolen credit cards and identity documents.
>
> We meet the leader, a 20-something American business student who set-up a website to bring together buyers and sellers of stolen cards and data. We see several levels of ShadowCrew management, including "moderators" who host online forums to help members design convincing phishing emails, and to plant spyware on users' computers to steal passwords and account numbers.
>
> We meet the "reviewers," who rate the stolen information for quality and street value. There are "vendors" who package the goods for sale to gang members, often through online auctions. Everyone moves quickly and talks fast, since stolen cards have to be used before cardholders cancel their accounts.
>
> Then, cut to a nighttime scene in downtown Washington, where a team of Secret Service agents are using high-tech surveillance tools to monitor the gang, who's having an online group meeting. We hear the "Go!" order, and armed agents break-down doors to a dozen homes and apartments around the country. Some weapons are uncovered, and one gang member jumps from a second-story window, only to be apprehended by agents on the ground.

> As the credits roll, the narrator says, "*The events you have seen are true...*" The ShadowCrew bust really happened, on October 26, 2004[4].

This ShadowCrew episode reminds us that thieves are behind every fraudulent charge and credit account that's opened in someone else's name. And it demonstrates that identity thieves are professional, organized criminals, capable of large-scale operations: the Secret Service found 1.7 million credit card numbers, access keys for 18 million email accounts, and identity data for thousands of people in their ShadowCrew investigation.

ShadowCrew harvested much of their data by phishing, where consumers were duped into giving up their own information over the phone or online. But they also hacked into a dozen corporate systems, including banks and credit card networks.

Today, the ShadowCrew gang members are being prosecuted under the Computer Fraud & Abuse Act, which carries prison sentences up to 20 years. We need more high-profile prosecutions like this if we want to have any hope of deterring identity thieves and reducing the losses due to credit card fraud and identity theft.

Business Bears 90% of the Costs of Identity Theft

Obviously, card fraud artists and identity thieves are spending other people's money. In 2005, Tom Lenard and Paul Rubin of the Progress & Freedom Foundation helped us understand who is paying for 55 billion dollars in annual identity theft losses.[5] Nearly all of these losses happen through the misuse of credit accounts, which occurs in two ways:

> Two thirds of these incidents are someone running-up charges on a victim's credit card. In these incidents, the cardholder incurs an average of $160 in out-of-pocket costs, and spends about 15 hours refuting charges and canceling compromised accounts. The retail businesses who accepted the fraudulent charge incur another $2,100. The loss differential between the cardholder and businesses is no surprise, given that nearly all card issuers limit cardholders' exposure for fraudulent charges. But the cost borne by retailers—many of whom are small businesses—is not often acknowledged when discussing identity theft.

---

[4] Brian Grow, Jason Bush, "*Hacker Hunters: An Elite Force Takes on the Dark Side of Computing*", BusinessWeek Online, May 30, 2005 http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

[5] Thomas Lenard and Paul Rubin, "*An Economic Analysis of Notification Requirements for Data Security Breaches*", The Progress & Freedom Foundation, July 2005 http://www.pff.org/issues-pubs/pops/pop12.12datasecurity.pdf

The remaining third of identity thefts involve someone opening new credit accounts in the victim's name. On average, the person victimized incurs $1,180 in out-of-pocket costs, and spends 60 hours clearing up the mess (although it can take years to clear one's credit record). On average, the businesses that issued or accepted the bogus credit are out by $10,000 each.

Lenard and Rubin report that total costs of $55 billion are borne by both business and consumers, with business incurring $50 billion, or ten times as much as the consumers who are victimized. In no way does this diminish the personal hardships of identity theft that can be devastating to individuals and families –victims can spend hundreds of hours dealing with the damage, and it may take years to clear their name and credit records. But the fact that businesses are hit with ten times as much as consumers explains why business is genuinely committed to reduce the losses due to identity theft.

We've been talking so far only about out-of-pocket costs and time spent by victims, whether business or consumer. The marketplace also imposes substantial costs on businesses that have apparently failed to secure the information entrusted with them. Businesses that lose customer data are punished by the marketplace, as customers leave and competitors pounce on the opportunity posed by a damaged reputation. The Ponemon Institute released a survey of 10,000 adults, drilling into their reactions to security breach notices they've received:

- 20 percent terminated their relationship with the company whose systems were breached.
- An additional 40 percent are considering whether to end the relationship.
- Five percent hired legal counsel after receiving a security breach notification. Up to 50 million Americans who have received notifications, posing a growing risk of lawsuits.

Of course, some breaches occur at businesses that serve other business customers, and don't deal directly with consumers. But large customers are also showing they will terminate relationships with vendors who've been breached, as seen with the CardSystems incident in 2005. It's clear that in choosing where to do business, customers are increasingly asking whether they can trust a business to maintain their data.

THE SMALL BUSINESS PERSPECTIVE

Small business doesn't often come to Congress to request new regulation. But irresistible forces have pushed 35 states[6] to enact their own breach notification laws, leading many businesses to call for a national notification standard. Congress, however, is inclined to combine a national notice requirement with data protection regulation that would extend to small businesses not currently regulated by federal agencies.

The State Stampede to Require Breach Notification

For the past three years, I've worked with businesses of all sizes to educate state lawmakers regarding security breach notification legislation. While not calling for new laws, most businesses acknowledge there are potential benefits to requiring notice of data security breaches:

- The requirement to notify provides an additional incentive for businesses (and state agencies) to tighten-up their information security practices, thus avoiding the embarrassing and expensive consequences of acknowledging a breach. Even businesses in unregulated industries appreciate the risks they face from lawsuits for actual damages occurring as a result of data security breaches.
- Notice requirements can include specific incentives to encourage businesses to use data encryption or other technological means to render data unusable if it's lost or stolen.
- Consumers who receive timely notice can monitor their credit accounts for unauthorized charges, add fraud alerts to their credit reports, and even request that credit reporting agencies stop new accounts from being opened in their name.

However, these potential benefits should be assessed for their likely effect and weighed against costs and unintended consequences:

- Notification by businesses only matters when it's a *business* that loses the data. Most identity theft and credit card fraud is done by *people* that the victim *actually knows*, so breach notification isn't even a factor.
- Over-notification will occur if consumers receive notices for situations that don't pose a risk of identity theft. And over-notification will de-sensitize consumers to situations of true risk if and when they occur. Most businesses have advocated a risk-based

[6] National Conference of State Legislatures website, at http://www.ncsl.org/programs/lis/CIP/priv/breach.htm

trigger for notice obligations, with incentives to safeguard data through practices such as encrypting or redacting sensitive data, or storing account information in a way that can't be linked with names.

- Businesses should be deemed compliant if they already follow notification requirements imposed by their functional federal regulator. Otherwise, these regulated businesses could be subject to conflicting requirements.
- Notice deadlines need to be realistic, given the time it takes to properly investigate the extent of a breach, verify addresses, and prepare informative and actionable instructions to consumers. Furthermore, regulations should be flexible as to how to communicate most directly and effectively with affected consumers.
- Drafts of some state notification bills created the risk of massive private lawsuits against companies who missed technical notice requirements. In one state, a business that missed a 15-day notice deadline on just 1000 consumers could be sued by plaintiff's attorneys for $1 million, under a provision of existing consumer protection law. State Attorney's General can certainly assess civil fines, and businesses are already susceptible to lawsuits for any actual damages incurred from identity theft or fraud based on data they lost. But there is little justification for empowering the plaintiff's bar to bankrupt a business for a technical failure to notify.

The most significant *unintended* cost of state legislation to require breach notification is that it has created an impossibly complex patchwork of overlapping and often conflicting laws.

An Impossible Patchwork of State Notification Laws

A rush to pass security breach notification bills has already created an unworkable system of inconsistent and incompatible state laws. It's confusing to consumers and makes it nearly impossible for businesses to comply. A small business with customer information from multiple state residents faces the challenge of simultaneously complying with as many as 35 state notification laws.

Consider the coverage of just one state notification law, Pennsylvania's Senate Bill 711, which was signed by Governor Rendell in December, 2005. Pennsylvania's law applies to any "*entity that maintains or manages computerized personal information*." Entity includes a "*state agency, political subdivision, individual or a business doing business in PA*". While there's no definition for "*doing business*" in this law, if a business has ever invoiced a

customer in Pennsylvania, it is likely to be subject to Pennsylvania's laws in notifying that state's residents of any lost or stolen personal data.

A patchwork of state regulation often prods industry to call upon Congress for a national standard that preempts state laws—something that's unpopular in state capitals. Ironically, however, state security breach laws are *preempting each other*, since most databases include customers from around the country. The only feasible way to comply with different laws is to follow the most restrictive parts of *any* state. For example:

> A business whose breached data included California residents would have to provide notice even when there's no risk of identity theft. Residents of other states with risk-based triggers would be alarmed to hear of the California notices in the media, so the business would have to give the California-style notice to residents of every state. Thus, California can preempt the risk-based trigger mechanism that has been adopted in many states.
>
> If any Illinois customers are among the data that was lost or stolen, Illinois law *doesn't allow a business to delay notification* while cooperating with law enforcement. So the required Illinois notice would compromise investigations being conducted by law enforcement officials in other states.

As you can see, some state laws are effectively preempting other state laws. Perhaps the FTC anticipated this concern with the final instruction of its publication, "Complying with the Safeguards Rule": *"Check to see if breach notification is required under applicable state law."*[7] Any business—large or small—that handles data from customers in many states needs a national standard to mitigate the patchwork of 35 state laws already on the books.

Congress is now weighing several bills that require both notice and data protection regulation, and the small business perspective on two leading bills is discussed below.

Small Business and Data Protection Legislation

Faced with an unworkable patchwork of state laws, a preemptive federal notice law would bring needed relief for business. Unfortunately, Congressional drafts go beyond notification requirements by imposing GLB-style data protection obligations upon small businesses not previously regulated by GLB.

[7] "FTC FACTS for Business, Complying with the Safeguards Rule", Federal Trade Commission, Bureau of Consumer Protection, Office of Consumer and Business Education, April 2006.

Data protection safeguard laws are a significant intrusion into the operations of small businesses, especially those in industries without oversight from a functional regulator. Not every business will need to build a brick house to protect against identity theft wolves, but business will have every incentive to overbuild to reduce regulatory risk.

Several House bills from the 109th and current Congress are related to notification and data protection:

- HR 3140 (109th) "Consumer Data Security and Notification ACT of 2005"
- HR 3997 (109th) "The Financial Data Protection Act of 2006"
- HR 4127 (109th) "The Data Accountability and Trust Act"
- HR 836 (110th) "Cyber-Security Enhancement and Consumer Data Protection Act"
- HR 958 (110th) "Data Accountability and Trust Act"

Four aspects of the small business perspective on these bills are presented next.

1. Many small businesses would be regulated for the first time

Some of these bills significantly expand which businesses are covered by data protection requirements. HR 3140 (109th) would treat previously unregulated small businesses as FINANCIAL INSTITUTIONS, with a definition that includes "*any person or organization that, in the regular course of business, collects and maintains written or electronic files containing individually identifiable information on customer transactions, including any bank, savings association, or credit union account number, credit card or debt card number, and any other payment account number, or any password, access code, or security code pertaining to any such account or any credit card or debit card.*"

Similarly, HR 3997 (109th) would encompass anyone "*maintaining, receiving, or communicating sensitive financial personal information on an ongoing basis for the purposes of engaging in interstate commerce.*" HR 4127 (109th) would extend safeguards and notification obligations to every person and business "*engaged in interstate commerce that owns or possesses data in electronic form containing personal information.*"

These proposed definitions could cover any sales or service business that records its customers' payment methods or stores any quantity of historical payment transactions. *That is, virtually every business that accepts anything other than cash.* Such a significant

expansion of regulation should be carefully constructed to help small businesses work their way into compliance, as described later in this testimony.

2. Requirements for breach notification should be predicated on risk of ID theft or fraudulent transactions

Consumers should be notified when data breaches pose a material risk of ID theft or fraudulent transactions, but Congress should avoid de-sensitizing consumers with over-notification, which has occurred with privacy notices required by GLB. Breaches that don't pose risks to consumers should therefore not drive notification requirements.

Most of the federal breach notice bills considered recently have advocated a risk-based trigger for notice obligations, and provided incentives for safe data practices such as encrypting or redacting sensitive data, or storing account data in a way that can't be linked with customer names.

For example, HR 3140 (109th) would allow businesses to reasonably conclude "that misuse of information is unlikely to occur" if the data were encrypted in accordance with the Advanced Encryption Standard adopted by the National Institute of Standards and Technology for use by the Federal Government.

However, incentives to protect data should anticipate that encryption is not the only mechanism that can effectively protect data, and that new means of protection will be offered in the future. HR 958 (110th) provides for such alternatives to today's encryption "*which renders data in electronic form unreadable or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data.*" And Senator Carper's bill (S.1260) provides an exception from notice requirements if lost data is maintained in an encrypted, redacted, altered, edited, or coded form that is not usable for purposes of identity theft or to make fraudulent transactions.

Breach notice mandates should include risk-based triggers and encourage the development and use of technologies to render lost or stolen data unusable when it falls into unauthorized hands.

3. State notification laws should be preempted by a national standard

As noted earlier, businesses now acknowledge the need for a national standard to replace a patchwork of 35 state laws governing security breach notification. Legislation considered in the prior and current Congress have offered differing degrees of preemption.

- HR 3997 (109th) contained broad preemption, overriding any state law that regulates the security or confidentiality of consumer information, safeguarding requirements, and investigation or mitigation mandates for data breaches.
- HR 4127 (109th) superseded state regulation of information safeguards and notice for unauthorized data access.
- HR 958 preempts state laws that require security practices or breach notification.

The above bills contain preemption language that would effectively create a uniform national standard for data safeguards and notification. HR 3140, on the other hand, relied upon the preemption level of GLB, which allows states to add more stringent rules if they do not conflict with federal rules. In effect, GLB imposes a floor—but no ceiling—on state regulation, thereby allowing the present state patchwork to persist.

4. Huge penalties could be fatal for small businesses

HR 4127 (109th) created separate penalty schemes for safeguard and notification violations. For safeguard rule violations, civil penalties under HR 4127 were calculated by multiplying the number of violations by a fine of up to $11,000 per. Each day of noncompliance is treated as a separate violation. Penalties for violations of the notification rules are calculated in the same manner, except that each failure to send a notice to an individual is treated as a separate violation.

The multipliers in these notification penalties could mean million dollar fines for a small business who fails to notify only a few hundred consumers. One can imagine the dilemma of a small business owner, upon discovering breaches that his employees should have reported much earlier. In that situation, an owner might avoid a multi-million dollar fine (and bankruptcy) by <u>not</u> reporting the breach, while hoping that it would not lead to any consumer harm. To avoid making this gamble too attractive, Congress should consider alternative ways to limit penalties for a single breach, and perhaps capping breaches that are discovered in a single investigation.

One other breach notification bill holds a nasty surprise for small business. The Cyber-Security Enhancement and Consumer Data protection Act of 2006 (HR 5318 in the 109th) would have made it a criminal offense to fail to report any "major security breach" to law enforcement. For private companies, a "major security breach" is one where "*personal information pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired.*" Owners of small businesses that are not currently regulated would be surprised to learn they face jail terms for failing to report "non-crimes", such as the accidental loss of a portable memory stick or a laptop computer. This bill would require notification of law enforcement when network intrusions are recorded by security monitoring software, without knowledge of whether any personal information was acquired.

GLB-style Safeguards Won't Work for Small Business

While federal legislation would provide relief from the patchwork of state data security laws, this relief could be costly to small businesses if GLB-style data safeguard requirements are imposed on industries not currently regulated by GLB. At least one bill in the 109th Congress (HR 3140) would have imposed GLB data safeguard rules on virtually everyone who maintains any customer account information. In fact, the pain of regulation could exceed the gain of preemption if these data safeguards are unworkable for small business.

At a fundamental level, data safeguard rules may not be justified since businesses already have powerful incentives to protect their customers' data. Legal liability and mandatory notification alone are probably sufficient to discipline businesses that fail to protect customer data.

Adding a data safeguard mandate will undoubtedly add compliance costs and carry unintended consequences, which should be evaluated against the positive effects of this regulation. Other members of this panel are better qualified to assess the effectiveness of the GLB Safeguards in place for the last several years.

Simply put, GLB regulates the handling of consumers' personal financial information, by financial institutions and also by non-traditional financial institutions, such as mortgage brokers and automobile dealers. However, GLB did not cover the vast majority of small businesses that would be regulated if new laws include anyone who handles sensitive financial information for purposes of customer billing and payments.

In 2003, the FTC began enforcing rules to implement the data protection provisions of GLB, known as the "Safeguards Rule".[8] As described in section 314.4 of the CFR (see Appendix B), the required elements of the Safeguards program included a risk assessment, monitoring and control measures. In its rulemaking, the FTC acknowledged concerns for small-entities and sought to "*preserve flexibility and minimize burdens*" on financial institutions subject to the rule.[9]

In the tradeoff between flexible standards and prescriptive requirements, small business will naturally favor flexibility. In technology fields, a one-size-fits-all prescription won't work for everyone on the day it's issued, and won't work for *anyone* as technology moves beyond the originally prescribed solution.

In these federal proposals, it's important to remember that "flexible" doesn't mean "optional". It means that requirements may be adapted to business operations and procedures. A "flexible" regulatory regime acknowledges that solutions may need to be adapted to work-around legacy software and customized in-house systems. However, flexibility in a regulatory standard can also prove confusing and unnecessarily drive up costs for small businesses:

- Small business owners won't be aware of new safeguard requirements if they are in an industry that has not historically been regulated. Many owners will learn for the first time that they are subject to new regulations when they see ads and pitches from software and hardware vendors, system integrators, and consultants –many of whom are ACT members. Each of these marketing messages will describe the problem and solution in different terms, depending upon the vendor's place in the "Security Stack" (Appendix A). Expect confusion and frustration among your small business constituents as they come to realize that they are subject to new regulations.
- Small businesses lack the expertise to select and manage the consultants and vendors needed to design and implement complex data security solutions. For instance, CFR 314(b) calls for a risk assessment, for which most small businesses will have to outsource to an experienced consultant. Most consultants who perform a risk assessment will naturally follow-up with a proposal to mitigate the risks, as a business is required to do under CFR 314(c).

---

[9] *Standards for Safeguarding Customer Information*, 67 Fed Reg 36484 (May 23, 2002).

- Conscientious systems consultants will propose a range of solutions with multiple degrees of data protection. Some proposals will be heavy on up-front costs, while others will spread costs over a long-term service agreement or outsourcing contract. With some costs, the size of small businesses will work to their disadvantage. Data encryption technologies, for example, cost roughly the same for databases with 10,000 records as for 10 million records.

Small Business Needs Flexible Standards plus Best Practices

If flexible standards can be confusing and expensive for small business, what's a better way to help small business implement data protection? ACT believes the answer is to stay with flexible standards, but call upon regulators to take it one step further. Require the FTC to seek, approve, and publish practical and affordable "best practices" that meet the flexible standard.

The FTC should look to industry for candidate best practices, since industry has the skills and incentives to implement approved solutions for regulated businesses. For example, leaders in the credit card industry responded to GLB Safeguard rules by developing a consensus approach for merchants who accept their cards for payment. Their Payment Card Industry Data Security Standard ("PCI Standard") is now part of the contract for any business that wants to accept credit card payments.[10]

Unfortunately, the PCI Standard is not simple enough to be a model for all small businesses. The current version is 12 pages long and sets forth 176 individual requirements grouped into a dozen major requirements. To be usable by previously-unregulated businesses, each requirement will need to be fleshed-out with specific examples of compliant behavior and/or specific product solutions.

Regulators should also be required to evaluate potential solutions for data protection compliance, and to publish an online catalog of results.

What we don't want to see is another "*Small-Entity Compliance Guide*" for Interagency Guidelines[11]. Though undertaken with the best intentions, this guide is of little

---

[10] www.visa.com/cisp

[11] "Interagency Guidelines Establishing Information Security Standards, Small-Entity Compliance Guide", at http://www.federalreserve.gov/Regulations/cg/infosec.htm

help to small business. It just reiterates FTC Safeguard Rules, without providing specific guidance on solutions for small business.[12].

These *Interagency Guidelines* are not likely to help small business owners to select and implement practical and affordable data protection solutions. There is much work to be done by regulators and by industry to reach that goal, which becomes essential if regulations such as the GLB Safeguards are applied to every small business who handles sensitive financial information for billing customers and booking payments.

Conclusion

We are grateful to this subcommittee for its continued vigilance on behalf of small business owners. As you consider data protection regulation, we ask that you act as our "angel" with House leadership and in conference committee.

Please use your significant influence to drive regulators to help small business understand and meet data protection standards without spending far more than they need to. Data protection standards should be flexible, yet regulators should quickly seek, evaluate, and approve multiple best practices that meet the standard.

Moreover, until regulators have published approved best practices suitable and affordable for small business compliance, please consider a temporary exemption from new data protection requirements for small entities—especially those businesses who were not previously covered by a federal functional regulator.

---

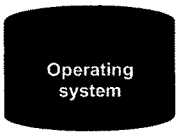
[12] Section 314.3 (b)(1), "*Standards for Safeguarding Customer Information*", 67 Fed Reg 36494, May 23, 2002. The Small-Entity Guide warns that "*Insurance coverage is not a substitute for an information security program.*"[12] Perhaps it was necessary to clarify that the FTC meant "*ensure*" when it actually wrote, "*Insure* the security and confidentiality of customer information

APPENDIX A: The Security Stack

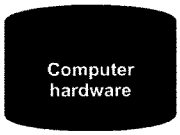
Responses to security threats happen at multiple layers of a "security stack" that starts with user behavior, includes hardware and software solutions, and rests on a foundation of network security.

User behavior and habits are security practices, ranging from the everyday behavior of employees to the top of IT management. This layer includes the acquisition, installation, maintenance, and application of updates. Users are fundamental to the security stack, since most attacks are facilitated by some aspect of user behavior. For example, 86% of respondents in a 2002 FBI survey reported an information security attack in the form of an e-mail attachment.

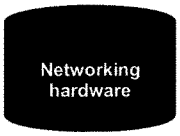
Application software includes productivity tools such as e-mail, word processors, spreadsheets, databases, instant messaging, browsers, firewalls, and anti-virus software. In the late 1990's, the application layer was often attacked with viruses propagating through vulnerabilities in e-mail clients or through macros embedded in documents.



Operating systems are the central layer of the security stack, both on client and server computers. On the client-side desktop environment, the Operating system layer includes Windows, Linux, and Apple. Server-side products include Microsoft Server, Sun Solaris, Novell, UNIX, and enterprise Linux. The server space has become the preferred target for malware makers seeking increased speed and scope of propagation.



Computer hardware includes desktop PCs, laptops, cell phones, PDAs, and pocket PCs. Although generally not the main target today, makers of these hardware devices are becoming more security-conscious. Industry efforts include processors with strong process isolation and sealed data storage devices.



Networking hardware includes routers and switches that serve as network gateways and firewalls that monitor incoming and outgoing traffic. This layer also includes an emerging device layer of appliances, offered by McAfee and other vendors that work to block spam and other suspect traffic to further augment security at the perimeter.

Networking transport & services is the layer outside our business walls. This layer includes packet monitoring and filtering by ISPs and Web infrastructure providers, who monitor Internet traffic, identify anomalies in the volume or nature of traffic, and act accordingly by notifying or blocking affected hosts and users.

APPENDIX B: FTC Safeguard Standards

16 CFR PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Authority: 15 U.S.C. 6801(b), 6805(b)(2).

§ 314.1 Purpose and scope.

(a) *Purpose.* This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) *Scope.* This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This part refers to such entities as "you."

This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§ 314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a

minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

From http://www.access.gpo.gov/nara/cfr/waisidx_03/16cfr314_03.html