AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DATA PROTECTION AND THE CONSUMER: WHO LOSES WHEN YOUR DATA TAKES A HIKE?

HEARING

BEFORE THE

SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

OF THE

COMMITTEE ON SMALL BUSINESS
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

WASHINGTON, DC, MAY 23, 2006

Serial No. 109–53

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

28–741 PDF WASHINGTON : 2006

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

COMMITTEE ON SMALL BUSINESS

DONALD A. MANZULLO, Illinois, *Chairman*

ROSCOE BARTLETT, Maryland, *Vice Chairman*
SUE KELLY, New York
STEVE CHABOT, Ohio
SAM GRAVES, Missouri
TODD AKIN, Missouri
BILL SHUSTER, Pennsylvania
MARILYN MUSGRAVE, Colorado
JEB BRADLEY, New Hampshire
STEVE KING, Iowa
THADDEUS McCOTTER, Michigan
RIC KELLER, Florida
TED POE, Texas
MICHAEL SODREL, Indiana
JEFF FORTENBERRY, Nebraska
MICHAEL FITZPATRICK, Pennsylvania
LYNN WESTMORELAND, Georgia
LOUIE GOHMERT, Texas

NYDIA VELÁZQUEZ, New York
JUANITA MILLENDER-McDONALD, California
TOM UDALL, New Mexico
DANIEL LIPINSKI, Illinois
ENI FALEOMAVAEGA, American Samoa
DONNA CHRISTENSEN, Virgin Islands
DANNY DAVIS, Illinois
ED CASE, Hawaii
MADELEINE BORDALLO, Guam
RAÚL GRIJALVA, Arizona
MICHAEL MICHAUD, Maine
LINDA SÁNCHEZ, California
JOHN BARROW, Georgia
MELISSA BEAN, Illinois
GWEN MOORE, Wisconsin

J. MATTHEW SZYMANSKI, *Chief of Staff*
PHIL ESKELAND, *Deputy Chief of Staff/Policy Director*
MICHAEL DAY, *Minority Staff Director*

SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

W. TODD AKIN, Missouri *Chairman*
MICHAEL SODREL, Indiana
LYNN WESTMORELAND, Georgia
LOUIE GOHMERT, Texas
SUE KELLY, New York
STEVE KING, Iowa
TED POE, Texas

MADELEINE BORDALLO, Guam
ENI F. H. FALEOMAVAEGA, American Samoa
DONNA CHRISTENSEN, Virgin Islands
ED CASE, Hawaii
LINDA SÁNCHEZ, California
GWEN MOORE, Wisconsin

CHRISTOPHER SZYMANSKI, *Professional Staff*

CONTENTS

WITNESSES

	Page
Kurtz, Mr. Paul, Executive Director, Cyber Security Industry Alliance	3
Sotto, Ms. Lisa J., Partner, Hunton & Williams LLP	4
MacCarthy, Mr. Mark, Senior Vice President, Public Policy, Visa U.S.A., Inc.	6
Lenard, Mr. Tomas M., Vice President for Research, Progress and Freedom Foundation	14
DelBianco, Mr. Steve, Vice President for Public Policy, Association for Competitive Technology	16
Dinham, Mr. Harry, President-elect, National Association of Mortgage Brokers	18

APPENDIX

Opening statements:	
Akin, Hon. W. Todd	25
Prepared statements:	
Kurtz, Mr. Paul, Executive Director, Cyber Security Industry Alliance	27
Sotto, Ms. Lisa J., Partner, Hunton & Williams LLP	34
MacCarthy, Mr. Mark, Senior Vice President, Public Policy, Visa U.S.A., Inc.	38
Lenard, Mr. Tomas M., Vice President for Research, Progress and Freedom Foundation	43
DelBianco, Mr. Steve, Vice President for Public Policy, Association for Competitive Technology	70
Dinham, Mr. Harry, President-elect, National Association of Mortgage Brokers	88

DATA PROTECTION AND THE CONSUMER: WHO LOSES WHEN YOUR DATA TAKES A HIKE?

TUESDAY, MAY 23, 2006

HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT
COMMITTEE ON SMALL BUSINESS
Washington, DC

The Subcommittee met, pursuant to call, at 10:00 a.m., in Room 2360 Rayburn House Office Building, Hon. W. Todd Akin [Chairman of the Subcommittee] presiding.

Present: Representatives Akin, Sodrel, Westmoreland, and Musgrave.

Chairman AKIN. Good morning, everybody, and thank you so much for coming to join us for the hearing this morning before the Regulatory Reform and Oversight Subcommittee of the Small Business Committee. And I am also pleased that some of you came some distance to be able to testify, and we are very thankful for that commitment.

We are going to be talking about who loses when your data takes a hike, and I want to especially thank all of you for the time you have taken to participate in this hearing.

We live in an age where information is as valuable as currency. It is now a commodity shared widely among different organizations in order to generate revenue. Data mining, data collection and targeted marketing are now very big businesses. These practices greatly affect small business because they improve the speed and accuracy of business transactions. Unfortunately consumers and businesses alike increasingly face many risks dues to information loss. These risks stem from the negligence of the firm, unethical practices of the firm's employees, and outside criminal activities.

A firm is said to be negligent when they do not employ good practices in handling consumer data. The most common form of data loss results in data being mistakenly lost, such as the loss of a laptop computer, blackberry, cell phone, or some other type of portable electronic device.

In most cases, this form of data loss does not result in any harm to the individual to whom the data belongs.

Another form of risk arises from employees of a firm using consumer data for their own gain. This is commonly referred to as "insider crime." A common example of insider crime is an employee

stealing consumers' credit car information and making purchases for themselves.

Finally, risk stems from criminals who operate outside the boundaries of the company and steal consumers' identity to make money. In the old days a criminal would have to gain physical access to paper files in order to steal consumers' identity or commit fraud. Today, because of greater information sharing, criminals can now gain access to the same information from the other side of the world. Although this is the least probable form of data loss for a company to incur, it is the most widely portrayed example by the media.

As incidents of large data security breaches pervade the newspaper headlines, states are moving quickly to protect the rights of their citizens. Twenty-nine states have passed data breach notification laws and many more are considering legislation requiring companies to notify consumers of a possible loss of their personally identifiable information. These regulations affect many companies that store or transmit personally identifiable consumer information.

Currently companies that sell across state borders are forced to understand and comply with these various state laws. This can be particularly onerous for small businesses. As Congress seeks to address the protection of consumers' personal information through legislation, lawmakers must consider the degree to which compliance is encouraged relative to the amount of economic burden placed on businesses.

We are here today to better understand the cost of complying with current state and federal law not only in the formulation of a data security policy, but in managing the necessary paper trail to prove compliance.

In addition, the Subcommittee seeks to understand the effect any new overriding federal law will have on data security compliance costs for small businesses.

Finally, we hope to determine whether special consideration for small businesses in the formulation of baseline provisions in a data security bill is appropriate. I look forward to hearing the testimony of the witnesses to learn more about how data security regulations can affect small business.

I would normally yield to the gentlelady from Guam, Madame Bordallo. However, she is not here today and will not be able to join us. So we will go directly to our witnesses. As I think the comments I just read state, our concern is that if Congress rushes too quickly on things, many times we overreact. An example of this is a bill called Sarbanes-Oxley. Many of us came to Congress because we hated red tape, and we ended up finding out that the enemy was us and we just made it worse, and that is the primary concern of this Subcommittee. We are concerned personally about identity theft, but we are also concerned that we making the regulations that are much, much more extreme than small businesses can afford. So that is the balance and the debate.

I am going to start by calling our first witness. Paul Kurtz, you have joined us before, sir, and we are glad to have you again. Paul is the Executive Director of Cyber Security Industry Alliance out of Arlington, Virginia.

Paul, you know the rules around here. We go by five minute intervals. At the five minute mark, the light turns red and the seat goes through the floor. You know the drill. We have a total of six witnesses today. We will do two panels of three. It gives me a chance to ask some questions, than other people come in, and they can ask questions. Then we will bring the next panel of witnesses up.

Paul, please proceed.

[Chairman Akin's opening statement may be found in the appendix.]

STATEMENT OF PAUL KURTZ, CYBER SECURITY INDUSTRY ALLIANCE

Mr. KURTZ. Great. Given my voice today, I think the five minute rule should not be much of a problem

First of all, thank you for calling this hearing. I think it is important, and I want to commend you for holding the town hall meeting you had in St. Louis last month, which I think is a vital part of outreach to small businesses in helping them increase awareness.

Laura, with me today is putting up a couple of slides from a survey that we are releasing today at the Cyber Security Industry Alliance, which I think is germane to the topic at hand: consumer confidence or voter confidence in the overall Internet. We have a substantial number of the population that are concerned about making online purchases, and a slide down below that you will see talks about the number of folks who think we ought to have new laws passed on the order of 60 to 70 percent when a population wants to see new laws passed to protect sensitive personal information.

In turning to small businesses, the Internet has enabled small businesses to compete with large business enterprises because of the accessibility and ease in communication the Internet offers, but this accessibility has also created new challenges by increasing threats to small businesses.

There are several reasons why or there are several things we think government can do to help improve the security of small businesses. First of all, the Congress can pass a national data security bill. We think that is very important for a number of reasons.

First and foremost, as you mentioned in your opening statement, at least 29 states have passed laws already requiring notification to consumers in the case of a breach of certain personal information. Four of those states have also included provisions that require security, reasonable security measures. What the Congress is contemplating is if you will both. It is putting in place those reasonable security measures across the board basically. All of the bills contemplated include that measure, and secondly, the notification piece. In the absence of a national bill, small businesses will be left to comply with the myriad of laws and regulations.

For example, if you have a small business in Missouri and you are on line, and you would subsequently have to comply with all of those state laws that have notification requirements or security requirements; so while it might be contrary to national thinking, having a national standard that applies to large enterprises, as well as small enterprises is important.

You might be tempted to, if you will, delay bringing in small enterprises into compliance with such a law. I would urge you not do so, that you support a national law right up front because if you delay the exemption, you are still going to be left with having to comply with the state laws that are on the books.

What will be important in any national law that is passed is obviously preemption, that it preempts all of the state laws that are in place, that the security measures that are put in place are strong, and as the data breach yesterday brings to light with 26.5 million names coming out or potentially exposed to identity theft, that we use encryption, not that the government must mandate the adoption of encryption, but the encryption as the best practice.

We are pleased to note that several of the bills on the Hill include encryption related provisions, in other words, as a best practice. We would urge that Congress swiftly move forward to pass a bill this year that includes reasonable security measures, preemption of state law with a risk based notification threshold and voluntary encryption measures.

Before I close, in the last 30 seconds I also want to note that the Executive Branch can take action as well. The Small Business Administration can do more. That is not to say that they have not done anything, but they can show a leadership role. They can form an advisory committee comprised with people from small businesses and others in the security industry and the private sector to advise SBA on where the gaps are and where the problems are.

They can also initiate a survey among small businesses to understand what their problems are, specifically what is inherent to exactly their problems.

And the final area that I would highlight that they can do is just as you started: more outreach. Engage in those local outreach efforts, those townhalls across the country. They have done some very valuable work with InfoGuard already. InfoGuard has chapters across the United States. They are built in. SBA with a new office could engage Infoguard more thoroughly and much more could be done.

And I will close. thank you.

[Mr. Kurtz's testimony may be found in the appendix.]

Chairman AKIN. Thank you, Paul.

I think that your comments were helpful, particularly in that you were quite specific of some things that need to be done. I appreciate that.

Lisa Sotto is a partner with Hunton & Williams, LLP from New York, and I think noted as one of the foremost experts on data security. We are just delighted to have you here, Lisa.

STATEMENT OF LISA SOTTO, HUNTON & WILLIAMS LLP

Ms. SOTTO. Thank you very much, sir.

This morning I will address three topics: first, state security bridge notification laws; second, information security requirements applicable to U.S. businesses; and, third, my recommendations for a federal security bridge notification law.

In 2002, California enacted SB 1386. It is because of this law that we know of the many information security breaches that have occurred during the past several years. The law requires organiza-

tions that own or license unencrypted computerized personal information about California residents to notify those individuals if the security of their data was compromised.

Since the spate of publicized security breaches in 2005, 29 other states have passed breach notification laws, and similar legislation is pending in 11 states. While the various state breach laws are similar in many respects, there are significant differences. In 15 states, for example, there is a harm threshold for notification. An entity that suffers a breach is not required to notify individuals if the entity determines that there has been no misuse of the information.

Another difference is in the definition of personal information. Typically personal information is defined in these laws as an individual's name plus Social Security number, driver's license number, state ID card number or credit/debit or financial account number.

In some states the definition is broader, for example, including date of birth. While most state breach laws cover only computerized data, some state laws also cover information in hard copy paper format.

Some state breach laws contain additional notification requirements, like the requirement to notify state agencies or credit reporting agencies of a breach.

Needless to say, the variations in the 30 state laws make compliance on a nationwide basis a complex matter.

I will now briefly outline the information security requirements applicable to U.S. businesses. First, Gramm-Leach-Bliley Act's safeguards rule requires that financial institutions maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards to protect customer information. These safeguards should be appropriate to the size and complexity of the entity, the nature and scope of the entity's activities, and the sensitivity of the customer information.

Another law that requires a formal comprehensive information security program is HIPAA. Like GLB, HIPAA adopts a flexible, scalable approach to information security. In deciding which security measures to use, a covered entity must take into account its size and complexity, its technical infrastructure, cost, and the probability of potential risks to the data.

A third information security requirement is found in California's AB 1950 and its state analogues. AB 1950 requires businesses that own or license personal information about California residents to implement reasonable security procedures to protect the information from unauthorized access.

Pursuant to the Fair and Accurate Credit Transactions Act, the FTC promulgated a rule in 2004 that requires businesses to take reasonable steps to guard against unauthorized access to consumer report information in connection with its disposal. Several states have even broader data disposition laws.

In addition, other laws create security obligations indirectly. For example, the FTC has applies Section 5 of the FTC Act to sanction what it believes to be inadequate security as an unfair business practice. Given the panoply of breach notification laws and information security requirements, a federal law that would preempt similar state laws is critical. Because data often flows beyond state

boundaries, a federal law would insure that personal information is subject to security requirements that are uniform throughout the nation and that affected residents of every state would be notified of a breach.

Such a federal law should require businesses that store sensitive consumer data to maintain reasonable security procedures to safeguard that data. With respect to breach notification requirements, I would advocate use of the California definition of personal information rather than an expanded definition. The California definition is narrowly crafted to include only information most commonly used by fraudsters to commit ID theft.

Since the purpose of breach notification is to inform individuals of events that might cause them harm, there is no need to expand the definition.

In addition, any federal law should contain a harm threshold requiring notification only if there is real risk of harm.

Finally, I would suggest that any federal law focus on computerized data. Only information maintained in electronic format could be subject to the high volume of harm these laws are specifically intended to combat.

With that I will end, and I would be glad to answer any questions. Thank you.

[Ms. Sotto's testimony may be found in the appendix.]

Chairman AKIN. Thank you, Lisa, and I appreciate your comments.

And next is Mark MacCarthy, Senior Vice President, Public Policy, with Visa U.S.A. from Washington, D.C.

Mark, thank you.

STATEMENT OF MARK MacCARTHY, VISA U.S.A., INC.

Mr. MACCARTHY. Thank you very much, Chairman Akin.

Visa appreciates the opportunity to testify at today's hearing on the important issue of information security in small businesses.

Visa is a leading consumer payment system and plays a pivotal role in the development of new payment technologies and services, including initiatives for protecting personal information and preventing identity theft and other kinds of fraud.

Visa commends the Subcommittee for focusing on the issue of information security and the incentives for small businesses to provide increased information security practices. Visa has long recognized the importance of strict procedures to protect cardholder information. Cardholder security is never just an afterthought at Visa. For Visa it is about trust. Our goal is to prevent fraud from taking place in the first place.

This commitment to fighting fraud includes Visa's zero liability policy. This protects Visa's cardholders from any liability for fraudulent purchases. Because the financial institutions that are Visa members do not impose losses for fraudulent transactions on the cardholders, these institutions incur costs when fraudulent transactions take place. These costs are primarily in the form of direct dollar losses, but hey also include card replacement costs, fraud monitoring costs, and incremental customer service costs.

Typically fraud losses are borne by the card issuer. However, rarely, if the merchant fails to follow proper authorization proce-

dures for face-to-face transactions, these costs may be passed back to the acquiring bank or to the merchant.

For Internet, telephone, and mail order transactions, merchants are generally responsible for unauthorized transactions. However, Visa provides merchants with a number of tools to prevent fraud and by using one of those fraud tools called "Verified by Visa," merchants can shift these fraud losses back to the card issuing bank.

Visa has implemented a comprehensive and aggressive customer information security program. It is called the Cardholder Information Security Program, CISP. This security program applies to all entities, including telephone orders, Internet brick and mortar, whether operating through the Internet or through any other channel of commerce. It includes not only data security standards, but also provisions from monitoring compliance and sanctions for failure to comply.

Visa has been able to integrate CISP into the common set of data security requirements that are used by all of the credit card companies, which is known as the payment card industry data security standard, or the PCI standard.

Visa also provides sophisticated neural networks that flag unusual spending patterns for fraud, and these neural networks enable our members to block transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institution and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in these cards, we again notify the issuers, and they begin a process of investigation and evaluation to determine the need for any card reissuance.

In addition to CISP and these neural networks, Visa has implemented a variety of additional security measures that are designed to detect and prevent fraud transactions, Visa's address verification service. It matches shipping and billing addresses. Visa maintains an exception file comprised of account numbers of lost or stolen cards, and we check account numbers against this exception file at the time of a transaction.

We have a card verification value, which is a unique three-digit value that is in the magnetic stripe of every single credit card and debit card. It insures that a valid card is present when you have a face-to-face transaction.

The CDV-2 is a unique three-digit code on the back of the credit card. It helps online merchants and telephone merchants verify that the card is really in the possession of the person who is conducting the transaction.

And Verified by Visa, which I mentioned before, allows merchants to avoid charge-back costs by having cardholders authenticate themselves while they're shopping online.

Advanced authorization is a new service that we are providing. It provides an instantaneous analysis of the potential for fraud at the time of the transaction itself. As a result of these measures, fraud within the Visa system is at an all time low of five cents for every $100 worth of transactions.

In addition, Visa and the U.S. Chamber of Commerce have announced a nationwide data security education campaign that will involve both the payment industry and merchants in the fight to

protect cardholder data. We believe that everyone who is involved in the payment system, Visa, financial institutions, processors, and merchants, have a shared responsibility to protect cardholder data.

On legislation, let me quickly summarize many of the things that Lisa mentioned we are in favor of as well. We do want a national notification standard. It has to be risk based. We do believe that there should be national requirements for reasonable security procedures. We think that there should be sufficient flexibility built into those national standards to allow for the needs of small business to be accommodated.

In particular, we think the size of the business needs to be taken into account whenever a federal agency forces these rules, as well as the nature of the risks involved. That kind of flexibility can insure that small businesses would be covered by the standard, but would be in a position where they could be afforded sufficient flexibility to come into compliance in an appropriate time and fashion.

[Mr. MacCarthy's testimony may be found in the appendix.]

Chairman AKIN. Thank you so much, Mark, for your testimony.

We have been joined by two of my good friends, Ms. Musgrave from Colorado to my immediate right, Mr. Sodrel from Indiana.

And we have been talking about, in a sense, a balance here for small business regarding the cost of overhead for small business relative to the questions of data security, and specifically two things. One is the reporting if you lose some data, and then second of all, what are the procedures you have to do to protect your data.

We have a total of six witnesses. The witnesses so far are making a strong case for the fact that a national standard would be helpful because each state has their own different separate rules and it would make it easier for business and commerce to comply with a national standard.

Mark, hearing what Visa is doing, and I have a Visa card in my wallet and appreciate it and everything; on the other hand, that does not strike me as small business. I do think about some guy that has got a cleaners or whatever it happens to be, the local store corner, and he needs a data security officer, and he needs a computer system that is approved by this and that. You know, we could just basically kill the poor small business guy with some of these rules and regulations. So that is a tension.

Mr. MACCARTHY. Can I comment?

Chairman AKIN. Yes, you can. This is a question and answer. So go ahead.

Mr. MACCARTHY. The local dry cleaner, you know, accepts Visa cards, but there is a fact about his system which is important and which limits his exposure to data security problems. Most of the small businesses, your local dry cleaner, for example, do not link their point of sale terminal to their cash register, and when of the factors that means that they typically do not save the data in the transaction after the transaction has taken place.

So they do not have the kind of large cardholder databases that are an attractive target for data hackers. Now, they still have to keep their information secure.

Chairman AKIN. Could you just clarify that a little bit from a systems point of view? When I go to the local cleaner down here at the bottom of the Longworth Building, you know, they get your

phone number or something or other, but if you want to pay it, I usually pay cash, but if you pay it with a credit card or something, you are saying they do not maintain that credit card number connected with my name?

Mr. MACCARTHY. They typically do not record that credit card number containing your name. Now, your bank will.

Chairman AKIN. So in that regard it is almost like a cash type business and, therefore, they would have very little liability. Is that what you are saying?

Mr. MACCARTHY. Yes. The information is typically not stored at the merchant level. It moves through the system. The bank that works with the merchant will typically store the information. The bank that works with you as the cardholder will typically the information, but the small merchant typically does not.

Chairman AKIN. Okay.

Mr. MACCARTHY. Now, if they do save the information, then all of the Visa security standards do apply, and as some small businesses get larger and they move from the small business to a medium size business, they tend to link their point of sale terminal and their cash register, and then they save the transaction information along with the cardholder information.

Chairman AKIN. This is when those kinds of laws would kick in then.

Mr. MACCARTHY. That is when it would kick in. It is at that stage. The vast—

Chairman AKIN. You see, in our congressional office, I am going to get personal about this. There are people who make contributions to my account using a Visa card, Visa numbers or Mastercard or whatever it is. What you are saying is as long as we destroy those numbers after that transaction goes through, it would not affect us.

Mr. MACCARTHY. The risks involved for the merchant at that point are minimal, and most of the small businesses in the country, we have five and a half million merchants, most of those small businesses are not in the position where they save the information after the transaction has taken place.

Now, the rules do apply, and if they do become larger, they will have to take the appropriate security steps to make sure the information is kept safe and secure, but we do not think that the burden on the small business that does not save the information is exorbitant at this point, and we would hope that national information as it moved forward would allow the Federal Trade Commission or whatever other national entity is involved in this sufficient flexibility to say that is a small business. The risks are not very large. They do not save the information. We do not need to have them hire a security officer. We do not need to have them do a security scan every year. They should not have to pay $100,000 for an expensive security audit.

And our private sector system already allows for that kind of flexibility right now.

Chairman AKIN. And then the other thing I think I heard all of you make the comment that the reporting requirement should be proportional to what the level of risk is. So if your computer falls in the ocean when you are going across something like that, you

do not need to worry about that particularly, whereas if somebody has come in and literally stolen that information, then you would have a more onerous reporting requirement.

Now, the reporting requirement, so what? I happen to be one of those 26 million people in the veterans' thing. Okay? And I find out that they have my name and Social Security number and birthday or whatever it is. What do I do? Does it do me any good to know that somebody stole it? Can I take any precautions as a consumer?

Mr. KURTZ. Again, may I?

Chairman AKIN. Whoever wants, yes.

Mr. KURTZ. In the first place, I would go back to the point that to me there is a realization that we need to come to in our society about the portability of vast amounts of information, and the need to take security more seriously in the recognized tools that exist today, including encryption. They have a laptop or the disk. The disk involved in the event involving VA, if it was encrypted, you would not be having the flash of news that we have today because VA could report that do not worry; it was stolen, but it is encrypted and the chances are incredibly low that—

Chairman AKIN. Is encryption pretty expensive or not really?

Mr. KURTZ. In fact, encryption technologies have changed over the past several years. So they are, if you will, more seamless and easier to apply. Under the PCI standard, PCI standard that Mark made reference to, they encourage encryption as well. I think if we were to ask this question of ourselves, you know, four or five years ago, it would be more difficult. It would have been difficult to implement.

To answer your question more specifically about, you know, all right, so I am notified; how does that help me? Well, one, you know, it allows you to at least understand and to look into your credit report, and now as a citizen you are entitled to free access to your credit report, I believe it is, once or twice a year. So you can at least put a flag out and look at your financial statements more clearly than you would in the past.

There are also other services that are out there. The people that organizations are supplying that help with ID theft assistance that come with home mortgages and all of those kinds of things. So the market is, if you will, coming to the problem and providing solutions for people and providing guidance.

And the final point I would make is, you know, organizations like the National Cyber Security Alliance who I believe testified here a month or ago has tips out there for what people can do if they think they are a victim of identity theft.

Chairman AKIN. Okay. I have run out of time. I have got to follow my own rules, but we have got time for other questions. I think, Mr. Sodrel you were here first and slightly edged out Ms. Musgrave, yes, if you would like to proceed.

Mr. SODREL. Thank you, Mr. Chairman.

Mark, you were say that if the law was sufficiently flexible, it would give the regulators an opportunity not to regulate. It has been my experience that bureaucrats have a tendency to err on the side of more regulation, not less regulation. It is called job security, you know, more people, more budget, bigger building.

So I would probably be inclined to work something that is relatively inflexible so that they do not have that opportunity to grow their business, if you will, and the business of regulating. I mean, I do not want small business to be put at the whim, if you will, of a regulator by passing something that has enough elasticity that they can overreach. So I would like to think in terms of how do we prevent over regulation.

If you have any comments along those lines because I think that is a bigger risk than not enough regulation.

Mr. MACCARTHY. There are two ways. If it is the Federal Trade Commission, there are a couple of ways in which I think they can be prevented from engaging in over regulation, but, frankly, I think the danger that they would reach down to the local dry cleaner is pretty minimal.

I mean, there are five and a half million merchants out there who accept Visa cards. They cannot go after every one for trivial violations of some rules. What they have done in their current actions is they have found the cases where it is large companies who have clearly violated the most minimal, basic security rules. they have not encrypted the data or otherwise protected it. They have saved security codes that they should not have saved. They have not had passwords, they do not monitor their systems. They do not do scans of their systems, and they have lost large amounts of data and millions of people have been adversely affected.

They focused their scarce resources on those kind of cases. So I think that should continue, and if there is any questions about the overreaching of their authority to affect small businesses in a way that does not make any sense from the public point of view, then I think there are two ways of getting at them. One is oversight hearings. I mean, the committees that have authority over these people should bring them in and say, "What are you doing? Why don't you do a better job of administrating your own scarce resources?"

And the other is the Appropriations Committee where you can say to them, you know, if you want to spend money on this stuff in this area, spend it on places where the risks are real and not on the areas where the risks are minimal. My sense is that you have to write it into the national standard that they have to take into account the size of the business and the nature of the risks. That has got to be in the national standard, and that gives you enough statutory flexibility to go after them in an oversight sense to make sure they do not overreach.

Ms. SOTTO. If I can add to Mark's comments, traditionally we have seen in privacy and security legislation in this country a requirement that standards are flexible and scalable to the size and the complexity of the entity and the sensitivity of the data that the entity maintains.

The FTC and HHS in enacting regulations under GLB and HIPAA have been very careful to make sure that they're not imposing specific security requirements on an entity, but are in fact asking the entity to assess its own systems and determine what is right for that size of entity given the data that is maintained.

I would expect that same sort of standard would follow in a new law.

Mr. KURTZ. I do not disagree with any of what has been said by the panelists. I think when you talk about how a statute is eventually crafted, one other point I would just add to the mix to keep in mind is that technology is changing so swiftly today that you want to build flexibility into the statute that allows technology to change because if you are too specific, then we have new mean available to people in order to secure themselves. Then if it is stuck in statute, then that inhibits innovation. It inhibits flexibility of small businesses even to perhaps deploy more efficient and cost effective security technologies for companies in the future.

Mr. SODREL. Thank you, Mr. Chairman.

Chairman AKIN. Thank you. Good questions.

Marilyn, have you got a question?

Ms. MUSGRAVE. Well, I apologize that I have not been here for the entire testimony. Could someone give me an idea when we talk about national standards? You know, we talk about how states vary, and I would like to hear some examples of where you think states have gone too far. Whether you name the state or not, I do not care, but in trying to find that happy medium when we are at a time where people have a very heightened concern about identity theft.

The Chairman mentioned, you know, the story about the veterans today. You know, in Colorado there was the Department of Motor Vehicle issue where, you know, information was sold. People were just incredulous, very angry.

So tell me when a consumer advocate group would look at this situation what would be a national standard that you think would be appropriate or national standards that would be appropriate?

Ms. SOTTO. If I may, some of the distinctions are problematic. I represent companies that need to notify individuals when they have breaches, and a breach, by the way, could mean a stolen laptop. IT could mean a laptop stolen from a home that has been burglarized, as has happened recently, yesterday. It was reported yesterday with respect to the VA.

A couple of distinctions that make it difficult to determine how to comply on a nationwide basis. First, the definition of personal information varies from state to state. There is a typical definition that follows the California definition, but there are a few states that include items like date of birth, and I can tell you that it is very difficult to steal somebody's identity with their name and date of birth, and in fact, that is very much public record information.

Other states include employee ID number, not meaningful when it comes to stealing somebody's identity, and by the way, when we talk about identify theft, that is a very broad range. It can mean account fraud where you get into somebody's financial information either through their bank account or credit card and do an unauthorized transaction or it can mean actually stealing somebody else's identity, taking the place of that person and taking out a loan, for example, or mortgage. So that is a very broad term.

Other distinctions. In some states you need to report to state agencies about the breach. So you have to deal with some states on a very specific and robust level. Other states could not care less about reporting specifically to them.

Another difference is that some states contain a specific number of days by which you need to notify individuals. That is a very difficult standard to meet when you are continuing to investigate and you cannot even quite pin down what happened.

So these distinctions make it very difficult when you are notified of a breach to figure out exactly how to comply with all 30, and it would really be enormously helpful to businesses of any size to have a national standard, and it would be very helpful, I think, to consumers as well, who would not be subject to the vagaries of these various state laws.

Ms. MUSGRAVE. Thank you very much.

Either one of you gentlemen like to comment on that?

Mr. MACCARTHY. Let me just jump in. I do think the reason to have a national standard has been explained by Lisa in pretty comprehensive terms. We support that.

The one item I would like to emphasize is this difference between account fraud and ID theft that she mentioned. In the VA incident, the Social Security number was taken. The name was taken. I do not think the address was taken, but I am not sure of that, and I do not know all of the details, but the risk there when your Social Security number, your name, your address, your date of birth, if all of that information has been compromised, the risk there is that someone can become you, can open up a cell phone account in your name or a bank account in your name or get a credit card in your name. They can become you and unbeknownst to you run up enormous amounts of debt in your name, which then will be reported to a credit bureau and you are going to have trouble clearing that up. That is a substantial risk.

When data is compromised from one of these cardholder databases which I talked about before, typically they get the cardholder number, the 16 digit number in the case of the Visa card. They probably get the expiration date, and they will also get the security code that allows them to make a counterfeit card.

With that they cannot become you. They cannot open up a new account in your name. What they can do is commit fraud, and so the risk there is not that someone will become you and open up an account to cause you indefinitely financial harm. The risk there is that someone will use your card to commit fraud.

We have zero liability. So the cardholder is protected in that circumstance. So what does this mean for policy? It means that in one case you might think carefully about the need to notify individuals that there is a problem and encourage them to do things like under federal law they have a right to put a fraud alert on their credit bureau account when they think that they have been a victim of identity theft. That is already in federal law, and probably they should do something like that to make sure that the people who use those credit bureaus know that there might be a problem here.

In the case of account fraud, our neutral networks will find that before they even know what is going on, will stop the transactions associated with that card, reissue a new card. That is not a good thing for the consumer. It is a bad thing, but it is a different kind of bad thing that full identity theft.

Chairman AKIN. Those were good questions, Marilyn, and thank you for clarifying the distinction there because that is a question

I had as we were going into this hearing. You know exactly what they are going to do with that data and what the uses are of it.

I assume the most common thing is to just rip somebody off, over the phone, give them a credit card number and buy a bunch of stuff, simple theft. Whereas you start getting more sophisticated when you go out and take a loan for a house or something.

Okay. We have got two panels. We have got three more witnesses. So I think what we will need to do is to move on to the next three witnesses.

Thank you, Paul, Lisa, and Mark, for joining us. If you would like to stick around, that would be good. Sometimes the members want to talk after the hearing, but I would like to kind of keep things on schedule.

Our next witness I believe is Tomas Lenard, Vice President for Research for the Progress & Freedom Foundation, Washington, D.C.

And, Tomas, I think we are going to get the new placards up there. We will go ahead with the same set of rules. You have got five minutes, and then we'll proceed to the other two witnesses and do questions.

STATEMENT OF TOMAS M. LENARD, PROGRESS & FREEDOM FOUNDATION

Mr. LENARD. Thank you very much, Chairman Akin. Thanks for the opportunity to testify today.

I am Senior Vice President for Research at the Progress and Freedom Foundation, and our mission at PFF is to study public policy issues that affect the information economy, and data security is surely one of the most important of those.

As has been mentioned earlier today, there are about 30 states now with data security laws and federal bills are moving through both houses of Congress. These new regulatory programs, like regulatory programs generally, should in my view be evaluated by weighing their benefits as against their costs.

To illustrate the benefit-cost approach to these issues, the testimony that I have submitted briefly summarizes an economic analysis of notification requirements for data security breaches that I recently did with Paul Rubin who is a professor of law and economics at Emory University, as well as an adjunct of PFF Fellow, and I have attached that to my testimony.

Very briefly, the major conclusions of the study are, first, that the annual cost of identity theft and related frauds are primarily borne by businesses, which gives them strong incentives to spend money on data security, and I think that was indicated by Mr. MacCarthy's testimony.

Second, the expected benefits to consumers of the notification requirement are extremely small and likely to be outweighed by the costs.

And because the notification mandate is dubious on benefit-cost plans, it should be targeted carefully.

And finally, federal preemption of state notification laws will reduce compliance costs and improve the benefit cost balance.

The effect of data security regulations on small businesses should be an important part of the benefit-cost calculus. These regulations

impose a per unit burden that is generally inversely related to the size of the company, which means that it is less likely that they will pass a benefit cost test when they are applied to small firms.

In addition, the added cost could have an adverse effect on competition because they make it more difficult for firms to enter markets in which the use of personal information is important.

There are a number of ways in which data security regulation disproportionately affects small firms. First, the requirement to establish a data security program involves costs, for example, specialized computer and legal expertise that are likely to be relatively invariant with the size of the firm and, therefore, hirer per unit of output for small than for large firms.

Second, establishing a safe harbor, for example, for companies that encrypt their data is also likely to disfavor small businesses because encryption is often quite expensive and its costs may not be sensitive to firm size.

Third, many of the costs of a notification program are also likely to be relatively fixed. Costs of some methods of notification, for example, posting a notice on the company's website or using the mass media may totally invariant with respect to the size of the breach, and this bias against small businesses is exacerbated by provisions that allow alternative notice if individual notice exceeds a size trigger.

And, fourth, without federal preemption, companies must familiarize themselves with numerous different state laws to make sure that they are in compliance, and the costs of this also do not vary much with firm size. So federal preemption, if enacted, will eliminate these costs and work to the advantage of small firms.

Finally, it is important to note that any regulation of the information sector that raises the costs of targeted advertising and obtaining accurate customer lists has a greater adverse effect on new entrants and small firms than it does on large, established firms. Established firms have lists of their own customers and visitors to their websites, but new firms must purchase such lists. As long as there is a healthy, robust market for customer lists and other such information, entrants can begin competing relatively easily.

All of this does not imply that data security regulations are necessarily a bad thing, but what I want to emphasize is the need subject then to rigorous benefit-cost analysis to assure that if they are adopted their benefits will be sufficient to outweigh their costs.

Thank you.

[Mr. Lenard's testimony may be found in the appendix.]

Chairman AKIN. Thank you very much for your testimony there, Tomas.

Our next witness is Steve DelBianco; is that correct?

Mr. DELBIANCO. DelBianco.

Chairman AKIN. DelBianco. Okay.

And, Steve, you are the Vice President of Public Policy for the Association of Competitive Technology from Washington, D.C.; is that correct?

Mr. DELBIANCO. Yes, if is, Mr. Chairman.

Chairman AKIN. Okay, and you know the drill and what the little lights indicate. When you get to the second one, that's a 30 second mark, right? Okay. Proceed, please, Steve.

STATEMENT OF STEVE DELBIANCO, ASSOCIATION FOR COMPETITIVE TECHNOLOGY

Mr. DELBIANCO. Chairman Akin, members of the Subcommittee, thank you for discussing the impact of data security threats and the impact of data security regulation on small business.

ACT, our group, is an advocacy group of more than 3,000 tech firms, small tech firms and E-commerce businesses, including many who handle the sensitive financial data associated with billing applications, but also those who handle payroll application. It is not just about billing customer credit cards. If you handle payroll information, you have got Social Security numbers as well.

I am also here before you today after making my own small business Odyssey. In 1984, I started an IT consulting firm in Northern Virginia, grew it to $20 million and 200 employees, and then sold the business before helping to start ACT. So I am a small business survivor.

Mr. Chairman and members of the Committee, I hope that you had a chance to see the new crime series, "CSI: Identity Theft." The premier episode featured a gang called shadow crew, and they made a science out of ID theft. They have got 4,000 gang members around the world working in an online marketplace to trade in stolen credit card, stolen document information, and personal data.

We meet the leader in this first episode who is an American business student and a few of his managers, who is a moderator who helps design convincing fishing E-mails to dupe people into giving up their personal information. There is another guy who designs spyware to get onto people's computers.

You meet these reviewers who take a look at the information they have stolen and figure out how they are going to charge for it or how they are going to sell it. Everyone on this episode, they talk fast, they move fast because they have got to use this stolen credit card information quickly before Visa or the card member cancers the credit card account.

Then in this episode they cut to a nighttime scene in downtown Washington where Secret Service agents are conducting a sophisticated surveillance of a gang member meeting. Well, the chief agent gives the go order and armed agents break down the doors, encounter some weapons. One of the perpetrators leaps out of the second story window only to be caught by an agent on the ground.

Well, as the credits roll in that first episode, you hear the narrator say, "The events you have seen are true," because this shadow crew bust really happened in October of 2004. The episode reminds us of something we have all lost sight of, I believe; that if a laptop is left in an airport or I leave one of these in the laundry, no ID theft has yet been committed. It takes a thief to commit identity theft. By using your card and fraudulently you're opening new credit accounts in your name. ID theft already has multiple victims, the consumers who have to go through great drama to get their credit cleared in the case of bad account, retailers and lenders. We heard Mark MacCarthy talk about the burdens on them, and the businesses who are pilloried for being sloppy with the data or, in the case of a disgruntled employee, takes off with a Rolodex. The business still is going to be pilloried for not having security provisions in place.

I would encourage you, please, let's not create a new set of victims by piling heavy regulation onto the backs of small business. Everyone knows, as Dr. Lenard said, that fixed costs disproportionately impacts small business, but there are some more subtle ways that small business is vulnerable, I think, to the regulation we're considering today.

One is that an owner's attention is stretched so thin. I was always far too busy fighting fires to spend any time preventing fires, although today you can bet that small business owners around the country are asking all of their employees what kind of data is on that laptop they take home. So fortunately they are paying attention to it today.

It is also very rare, as Dr. Lenard said, for a small business to have any in-house expertise in legal and IT security, and that means it is a very difficult for them to solicit, select, and then manage IT vendors and our source vendors to get the security implemented.

As this Committee well knows, this makes compliance awfully expensive for small business, as we saw in the case of Sarbanes-Oxley. I'm not as convinced as my fellow panelists today that we absolutely need new data protection regulation in order to make small business care about security, and I'm not actually convinced that that would actually reduce the incidence of ID theft.

But I am clear regulation is coming. You can feel the momentum coming, and there are some good reasons. Consumers can take measures to protect themselves if they receive notice of a breach just like we discussed with the Chairman, and also since states have created a patchwork of notice laws, we have got to have preemption for reasons others have discussed.

But Congress is looking not just at notice preemption. They're also eager to expand the data protection requirements, and that has made this a two-part discussion today. It's not just notice. It is data protection.

Now, the anticipated legislation could expand it to businesses that aren't even covered today, businesses that use any information for interstate commerce. Now, in regulating data protection flexibility is always better than a prescriptive solution, but flexibility does not mean that it is optional. A small business will not know where they are in terms of security unless they hire a consultant and pay for an assessment, and they probably cannot understand where they need to arrive even in a flexible standard because there is a range of different risk mitigation levels you can arrive at.

Small businesses, what they need are road maps. We need road maps to get from where we are to where we need to be under a flexible standard. Regulators should evaluate best practices in industry to decide which road maps can work for a small business. We could look to currently regulated industry for best practices, such as Mark MacCarthy described with the PCI data standard, and we can look to IT vendor, members of my group and Paul's group, to come up with best vendor solutions.

In closing, Mr. Chairman, I would say please remember who are the real criminals behind identity theft, and please don't overburden small businesses. Perhaps it is best to come right out of the gate with the kind of small business protection that was being con-

sidered down the stretch on Sarbanes-Oxley, and that is please consider giving small businesses a delayed implementation date for new data protection laws.

Go ahead and preempt notice immediately, but give a delay on data protection laws. Until there are enough approved road maps in place to get us from where we are to where we need to be.

Thank you, and I look forward to your questions.

[Mr. DelBianco's testimony may be found in the appendix.]

Chairman AKIN. Thank you very much, and I appreciate your perspective, Steve, as the guy who started your own business that way. The things that you articulated are very much the concerns of this Committee.

There are other committees that are working on these bills, but we're particularly concerned with the regulation's effect on small businesses.

We have been joined also by my good friend Congressman Westmoreland from Georgia. Welcome, and this is our second panel. We have one more testimony and then we will get around to some questions.

Our last witness is Harry Dinham, President-elect, National Association of Mortgage Brokers, Washington, D.C.

Harry, welcome to the hearing.

STATEMENT OF HARRY DINHAM, NATIONAL ASSOCIATION OF MORTGAGE BROKERS

Mr. DINHAM. Thank you, Mr. Chairman.

Thank you for inviting NAMB to testify today on the potential burdens placed on small businesses by proposed data security legislation. As the voice of mortgage brokers NAMB speaks on behalf of more than 25,000 members in all 50 states.

Identity theft remains one of the fastest growing crimes in America. Clearly, efforts to protect against identity theft are necessary and we commend Congress for taking action on this issue.

Equally important, however, is the awareness that proposed measures should not result in unintended harm to small businesses of America. I would like to discuss the lack of uniformity and clarity caused by the current patchwork of laws, credit freeze provisions, and the time and cost burdens placed on small businesses by any final monitoring provisions.

Today at least 30 states have enacted security breach notification laws. These multiple state laws create a regulatory framework that is unduly burdensome, costly and complicated for mortgage brokers that have limited resources and time, especially for those who operate in tri-state areas. NAMB believes that a uniform national standard will help small businesses protect their consumers' sensitive personal information effectively in a cost efficient manner.

Adding to the issues raised by this patchwork of state security branch laws is the recent trend of enabling consumers to lock their credit files, often referred to as credit freeze laws. Credit freeze laws are especially burdensome to small businesses. A credit freeze eliminates any point of sale transaction because it can take as many as three days to remove the freeze once the consumer has notified the consumer reporting agency to thaw the file.

Proposed legislation should not include a credit freeze provision because it inhibits small business mortgage brokers from accessing borrowers' credit report in time sensitive transactions. Moreover, an unintended consequence with these credit freeze laws is that small businesses are placed at a competitive disadvantage compared to financial institutions where the consumers have preexisting accounts. This is because preexisting business relationships are exempt from credit freeze.

For example, the mortgage division of a bank that the consumer already has a relationship with can still access consumer's credit file. This preexisting business relation exemption inhibits comparison shopping and reducing competition by limiting consumer choice to their existing bank.

Lastly, proposed legislation should not require small businesses to offer file monitoring. NAMB supports legislative proposals that would permit functional regulatory agency to exempt small businesses in a fair manner while at the same time protecting consumer interest. To aid the agency, Congress should incorporate statutory factors or guidelines that must be considered by the agency.

For an example, the legislation can provide that an exemption from the file monitoring required for mortgage brokers that are under certain size or have a limited volume of loans per year. At a minimum, NAMB recommends the file monitoring services be provided only if the consumer has already exercised their right to obtain their free credit report from each credit reporting agency for the calendar year.

Congress should also provide regulatory authority to place price gaps on the fees that small business mortgage brokers must pay to provide the service. In short, any proposed file monitoring provisions should be crafted so that it does not provide costly and unduly burdensome for the small businesses. To do otherwise would only increase consumer costs significantly.

NAMB supports federal legislation that establishes a uniform national standard for investigation and notification of data security breaches, but which is cognizant of the time and costs limitations that small businesses face.

NAMB believes that any proposed legislation must complement but not otherwise duplicate or override existing legislative and regulatory schemes that safeguard sensitive consumer information against identity theft.

NAMB looks forward to working with Congress to insure that any such proposed legislation balances the need of both consumers and small business. NAMB appreciates the opportunity to offer our views on the impact of current legislative proposals may have on small businesses.

[Mr. Dinham's testimony may be found in the appendix.]

Chairman AKIN. Thank you, Harry. I think you are one of the few that brought it in 30 seconds ahead of time. So good job.

I have got a question. Steve, if you were to take a look at from a small business point of view, which is a bigger threat, the reporting piece or the procedure piece, from a cost point of view for a small business.

Mr. DELBIANCO. Mr. Chairman, by "reporting" I think you mean the mandatory notice, right? In the case where there is a risk based trigger and there is an opportunity to provide the notice in a way that I am most customarily communicating with my customers, I believe that cost is far less than the procedural requirements for what we have been calling data protection requirements that would be imposed on small business.

Chairman AKIN. I guess it does vary. It probably depends on what the laws say and also what the situation is because the guy that lost the laptop with 26 million people on it, that reporting cost is going to be hefty, I would think; is that correct?

Mr. DELBIANCO. Yes, it would. Most, if not all, of the 29 states that have adopted notice laws though have provisions in there that if the cost or quantity of notice exceeds certain thresholds—I think it was half a million dollars in California—that there are alternative means of notification through public press releases, website announcements, newspaper postings.

Chairman AKIN. So you do not have to literally send direct mail to every single person.

Mr. DELBIANCO. You would if the numbers are below the thresholds. But when the numbers exceed the thresholds, there are alternative forms of notice.

Chairman AKIN. Okay. One of the issues that receives at least passing attention here in Congress is the question of immigration. If you are trying to establish one of the things that we have passed a bill in the House regarding a prospective employer, what he is supposed to do is to check when somebody comes the Social Security number against the name and the birthday. If you have those three things, basically you have established your identity for the purposes of that bill as a legal immigrant in order to work in this country.

What are the key pieces of information that are most necessary to misuse in terms of identify theft? What are the key pieces of data?

Mr. DELBIANCO. Mr. Chairman, as Lisa Sotto has indicated, if you got the Social Security number, full name and address record, you are in probably pretty good shape to begin to open a cell phone account, a credit account and begin to assume the identity.

Chairman AKIN. Do you need a birthday or not? Is birthday critical information? No, it is not. If it were critical, we would have an extra panel here.

Mr. DELBIANCO. If it were critical, you could look it up. It is part of the public records.

Chairman AKIN. Oh, that is right. Yes, because we do those automatic—I mean some politicians do birthday cards to people. So that is all public. That is right. Okay. Yes, so you do not even need the birthday. All you have got to do is get Social Security number and the right name, and then you are in business then. Okay. Good.

Let's see. Other questions? I think Mr. Sodrel is next.

Mr. SODREL. Well, I am only 16 months out of what I call real life. This is the first public office I have ever held, and I spent my life either being on the payroll or making the payroll. So I tend to have a little bit different perspective.

I do not know if you heard earlier when I talked about mission creep. When you build in too much flexibility in the law, the regulators tend to over regulate. They always want to err on the side of too much regulation rather than too little. I watched in our company. In my granddad's time, you had to have a truck and a license plate, and you were in the trucking business. Now you have to have an EEOC officer, an EPA officer, an OSHA officer, and ADA officer and a federal DOT compliance officer, and this officer and that officer which is not really practical for a small business.

So I am kind of concerned here that we are going to crate now information security officer in addition to all of the other officers for a five-person business. Particularly Internet businesses tend to be short on employees, maybe big on data, but small on people.

So any suggestion that you have to try to come up with something that is common sense, you know. I understand interstate commerce is difficult for a business to comply with 30 state laws. It may be appropriate to have federal preemption since we are in interstate commerce, but we need to do it in a fashion that does not overburden small business.

I am from Southern Indiana. We often call small business your seed corn. I mean if you follow the string back far enough every business was a small business whether it was Bill Gates or Microsoft or Lewis Chevrolet. So we do not want to completely stifle the growth of small business while we are trying to fix this problem.

So if you have got suggestions on how we keep it simply, how we do it in a fashion that makes sense and still small businesses can still survive, and Sarbanes-Oxley was a good example.

Mr. LENARD. I think I agree with everything you said, and I think you do point up kind of a tension there. It seems to me you do want to have some flexibility because you do not want to lock in procedures that really may not make sense, you know, that may make people spend a lot of money addressing problems where, you know, the risk is minimal or use technologies, you know, when they become outdated or when other technologies that are better or cheaper.

So I think you want to try to do both things. It is a challenge. You want to have flexibility to do something that really does make sense, but also, you know, limit the law so that it is not susceptible to regulatory creep of the type that you are concerned about because I think that is very legitimate.

I think, you know, the primary rationale at this stage for passing a law probably is federal preemption to get one law that you are going to have laws anyway. So you might as well have one, and then to try to put in sensible procedures that really do target, are precisely targeted as possible to address the situations where there is a real risk so that you really can get some benefits out of the law and not spend money where the benefits are minimal.

Mr. DELBIANCO. The Representative is also one who has signed the front of the paycheck before. I can sympathize with your prior life.

There are two issues to consider on preemption. The notice laws, the notification requirements, I believe it is a slam dunk, Representative, to make that a federal preemption. But on data protection, I think we have to be careful to watch for the trap that you

describe, the trap of flexibility coming out of Congress, turning into too much regulation by the regulator.

But I would point to GLB and the regulation pursuant to it as perhaps a better example than ones you have experienced before. Congress was very flexible in the instructions it gave to the FTC on GLB, and FTC, I think, has done an admirable job of coming up with equally flexible requirements that business can then meet.

However, I want you to be clear. Having been in the business myself, I know what happens when a vendor, a consultant, a systems integrator has an opportunity to tell a business whether and how it is compliant with something that is very flexible, and then after telling the business where your risk lies in your data protection practices, it is then up to me to adapt all of your business procedures, the scale of your operation and your business model to say, "Here is a solution that I can deliver for you that will meet the requirements of the law."

Now, a consultant might be inclined as I was to over engineer things, but again, both of us are going to be inclined to eliminate the risk not just manage the risk, but to eliminate the risk, and in that sense the solutions become very expensive. So flexibility from Congress to the regulators, flexibility from the regulators to industry is all working pretty well in GLB, but what I believe has happened is that the industry has only begun to deliver solutions that are compliant with that. We need more time for those solutions to be cooked down into road maps and best practices that are affordable and digestible for small businesses.

Chairman AKIN. I think that was a good set of questions. Just before I go to Congressman Musgrave, one of the comments that was made is I do not think the government is going to go after all of those different dry cleaners and small people. You know, the government doesn't have to go after all of them. They just have to ream one of them out and they have everybody scared to death and adding tremendous overhead to their cost of operations.

We see numerous examples in Congress. People, our constituents, complain to us about excessive regulation from the federal government and I have seen some really amazing examples. I think the recent one was where we have people that are building subdivisions in our area, and the drainage ditches in the subdivisions are being viewed as navigable waterways. Wasn't that innovative? I do not know who thought of that, but anyway, we have those difficulties.

Well, we now have my good friend, Marilyn Musgrave from Colorado.

Ms. MUSGRAVE. I was just looking over the section, Mr. Chairman, about file monitoring, and you know, certain presumptions there that reporting occurs, but then say, you know, that there are bad actors that don't do that, and I'm looking down here and my ears kind of perk up when you talk about price control and asking for more regulatory oversight from the SBA. So I assume it would fare better there.

So you actually want a price cap on what the mortgage broker can be charged for monitoring services. Could you comment on that, please?

Mr. DINHAM. Well, yes, ma'am. We really feel that, you know, we need to maintain our cost controls because we are in a small business. One to five people is our normal membership of our association, and anything we can do to hold our cost down is just a benefit to the consumer because everything that we have to do outside of that is going to add to the cost that we are going to have. It is going to be passed on to the consumer eventually. So anything we can do to control what it is going to cost us to do this monitoring would definitely be a benefit to the consumer.

Ms. MUSGRAVE. Do you think that changes in technology will affect the price of the monitoring, the cost of the monitoring?

Mr. DINHAM. I really do not know that it would change that, but you know, we have just seen things that would start out at a low price and they tend to edge up as it becomes more and more popular, and that is a real concern to us. We are very cost conscious as small business people.

Chairman AKIN. Lisa, you have been kind enough to stay around. If you would like to jump in on any of these questions just pretend like you are part of the immediate panel if you would like to. If you want to, yes.

Ms. SOTTO. The cost of credit monitoring actually varies quite dramatically depending on the leverage of the company, and I have worked with some companies that pay one price and other companies that pay a dramatically different price because they are big enough so that they have negotiating power, and they also have more leverage based on the number of enrollees who are anticipated in the credit monitoring.

Typically I have found that about five to ten percent of the number of names that have been breached will, in fact, enroll in credit monitoring. So the cost that the credit bureaus charge for the monitoring tends to be based on the volume and on the leverage that the particular company has with the credit bureau.

Ms. MUSGRAVE. That is why I was trying to figure out how a price cap would work. It seems very complicated to me.

Thank you.

Chairman AKIN. Does that conclude your questions?

Ms. MUSGRAVE. It does, and thank you, Mr. Chairman.

Chairman AKIN. Okay. Let's see. I had one more I was just thinking of. I am trying to remember what it was.

Does it make sense from a passing point of view to do the reporting piece of the bill separate from the other part of the bill? Does that seem like that it logically fits into two pieces from a legislative point of view?

Mr. DELBIANCO. Mr. Chairman, I would agree with that approach.

Mr. DINHAM. I would also.

Ms. SOTTO. Thank you.

It is interesting to me that California passed SB 1386 before AB 1950. It is backwards in a way. I think if you pass legislation that requires that you have a security program in place first, you would prevent the need to have notification requirements in at least some measure because if there are security fixes in place with respect to a particular database, there is less likelihood that that database will be vulnerable to attack and, therefore, less likelihood that you

will need to, in fact, notify individuals whose data might have been breached.

Chairman AKIN. I see the logic of what you are saying, but it also sounds like the predominance of testimony here this morning was because of the patchwork of various state laws, that there is almost a more practical sense a need for a federal standardization kind of procedure. That almost might be a simpler question and less expensive question than the second.

Ms. SOTTO. I think it is simpler, yes, but I don't think it really solves the problem. I think there really is a need for federal legislation. There is a dire need in the breach notification arena because of the patchwork of state laws, but I think I am dealing with a company right now that has encrypted all of its laptops. So they have done the right thing, but prior to encryption, which is, by the way, about $100 a laptop depending on the type of encryption technology you use; prior to encryption they had a dozen or so incidents of stolen or lost laptops that now need reporting.

So after the first one they knew to go ahead and encrypt, but they still had many more. I think if you impose security requirements, then you wouldn't have these multiple incidents of breaches that would require notification.

Chairman AKIN. Well, anybody want a last word on that? Maybe Steve.

Mr. DELBIANCO. Thank you, Mr. Chairman. While security requirements if enforced and affordable would reduce the incident of breaches, you can still be sure breaches would occur, and the state patchwork of laws would apply. We are dealing with laws that are inconsistent with each other.

Illinois, for instance, does not permit the delay of notice if you are working with law enforcement. So you might have Illinois residents in your database. That means that they have got to know right away, whereas the other states have allowed you to delay while you try to set up a sting operation to catch the bad guys.

In the case of New Hampshire, if you missed by a day the 15-day notice deadline to 1,000 customers, you are liable for a million dollar private right of action from the plaintiff's bar, and that is for a technical failure. We have a lot of concerns and need to solve it in the states right now, and even if we had data protection mandates that were followed, things happen. Laptops get lost, and we cannot pass a state patchwork of notice laws for much longer.

Thank you, Mr. Chairman.

Chairman AKIN. With that, the hearing is concluded. Thank you all very much for your testimony.

[Whereupon, at 11:14 a.m., the hearing was adjourned.]

W. TODD AKIN, MISSOURI
CHAIRMAN

MADELEINE Z. BORDALLO, GUAM
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
109th Congress
Committee on Small Business
Subcommittee on Regulatory Reform and Oversight
2361 Rayburn House Office Building
Washington, DC 20515-6315

Opening Statement
May 23, 2006
Regulatory Reform and Oversight Subcommittee
House Committee on Small Business
W. Todd Akin, Chairman

Good morning and welcome to today's hearing entitled "Data Protection and the Consumer; Who Loses When Your Data Takes a Hike?" I want to especially thank the witnesses for taking time out of their busy day to participate at this important hearing.

We live in an age where information is as valuable as currency. It is now a commodity, shared widely among many different organizations in order to generate revenue. Data mining, data collection, and targeted marketing are now very big business. These practices greatly affect small business because they improve the speed and accuracy of business transactions. Unfortunately consumers and businesses alike increasingly face many risks due to information loss. These risks stem from the negligence of the firm, unethical practices of a firm's employees, and outside criminal activity.

A firm is said to be negligent when they do not employ good practices in handling consumer's data. The most common form of data loss results in data being mistakenly lost, such as the loss of a laptop computer, BlackBerry, cell phone, or some other type of portable electronic device. In most cases, this form of data loss does not result in any harm to the individual to whom the data belongs.

Another form of risk arises from employees of a firm using consumer data for their own gain. This is commonly referred to as insider crime. A common example of insider crime is an employee stealing consumer's credit card information to make purchases for themselves.

Finally, risk stems from criminals who operate outside the boundaries of the company and steal consumers' identity to make money. In the old days, a criminal would have to gain physical access to paper files in order to steal consumers' identity or commit fraud. Today, because of greater information sharing, criminals can now gain access to the same information from the other side of the world. Although this is the least probable form of data loss for a company to incur, it is the most widely portrayed example by the media.

As incidents of large data security breaches pervade the newspaper headlines, states are moving quickly to protect the rights of their citizens. Twenty-nine states have passed data breach notification laws and many more are considering legislation requiring companies to notify consumers of a possible loss of their personally identifiable information. These regulations affect many companies that store or transmit personally identifiable consumer information. Currently, companies that sell across state borders are forced to understand and comply with these various state laws. This can be particularly onerous for small businesses. As Congress seeks to address the protection of consumers' personal information through legislation, lawmakers must consider the degree to which compliance is encouraged, relative to the amount of economic burden placed on business.

We are here today to better understand the costs of complying with current state and federal law, not only in the formulation of a data security policy but in managing the necessary paper trail to prove compliance. In addition, the Subcommittee seeks to understand the effect any new overriding federal law will have on data security compliance costs for small businesses. Finally, we hope to determine whether special consideration for small businesses in the formulation of baseline provisions in a data security bill is appropriate.

I look forward to hearing the testimony of the witnesses to learn more about how data security regulations can affect small business.

Prepared testimony of
Paul B. Kurtz
Executive Director
The Cyber Security Industry Alliance

Before the House Small Business Committee
Subcommittee on Regulatory Reform and Oversight
"Data Protection and the Consumer: Who Loses When Your Data Takes a Hike?"
2360 Rayburn House Office Building
Tuesday, May 23, 2006
10:00 AM

Introduction

Chairman Akin, Ranking Member Bordallo and other members of the Subcommittee, thank you for the opportunity to testify today before the House Small Business Subcommittee on Regulatory Reform and Oversight. My name is Paul Kurtz and I am the Executive Director at the Cyber Security Industry Alliance (CSIA). I will cover several areas in my testimony: the importance of data security to small businesses and steps small business, industry, and the Federal government can take to improve security.

Before I begin my comments, I would like to thank Chairman Akin and Ranking Member Bordallo for emphasizing the important role information security plays with small businesses through hearings such as this, and outreach efforts to discuss security with small business owners and their supporting entities. And to Chairman Akin in particular, CSIA was pleased to have representatives from three of our member companies participate in a Town Hall discussion you held last month in St. Louis. CSIA also worked with the National Cyber Security Alliance (NCSA) to produce a tip card for small businesses that was distributed at that event, and can be found on NCSA's website StaySafeOnline.org. We appreciate, and are supportive of your efforts to increase information security awareness, both here in DC and at home.

CSIA is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education, and awareness. The organization is led by CEOs from the world's top security providers who offer the technical expertise, depth and focus needed to encourage a better understanding of security issues. It is our belief that a comprehensive approach to ensuring the security and resilience of information systems is fundamental to global protection, national security, and economic stability.

Why Securing Data within Small Businesses is Important

Small businesses are the backbone of the American and international economy, as nearly 99 percent of all U.S. businesses are small or medium-sized,[1] and they represent 97 percent of all U.S. exporters.[2] The Internet has enabled small businesses to compete with large enterprise because of the accessibility and ease of communication the Internet offers; but this accessibility

[1] 2003 County Business Patterns. http://www.census.gov
[2] http://www.sba.gov/aboutsba/sbastats.html

has also created new challenges by increasing threats such as those caused by system vulnerabilities and exploitation by bad actors. As you know from the Subcommittee's hearing in March on "The State of Small Business Security in a Cyber Economy," Symantec Corporation found in its semi-annual Internet Security Threat Report that small businesses have consistently been one of the top three most targeted groups for cyber attacks over the past year.[3] Organizations with weaker security infrastructures - often small businesses with more limited resources – are exploited by cyber criminals in greater numbers.

Although small businesses have increasingly been targeted recently by cyber criminals, data security has been a front-page news story for well over a year now. Since February, 2005, when it was revealed that a major data broker disclosed personal data to criminals posing as legitimate businesses, more than 55 million records of Americans' private personal information – an average of 120,000 per day – have been hacked into, lost, stolen or otherwise compromised from digital databases.[4] In fact, more than 60 new major incidents have been reported since January 1, 2006. These security breaches are increasingly eroding public confidence in the security of private personal information. According to a survey CSIA recently released, 50 percent of Internet users avoid making purchases on the Internet because they are afraid their financial information may be stolen. This lack of consumer confidence inhibits e-commerce across the board, but the problem for small businesses is disproportionately greater. This is so because in the absence of reliable assurances that reasonable security measures are in place, consumers will assume, rightly or wrongly, that larger, better-recognized businesses will offer their customers more protective avenues of recourse in the event of a problem, while smaller businesses with little brand-recognition would offer no such intangible comfort level.

There are other important reasons why small businesses must take data protection seriously. For many small businesses that are part of the integrated supply chains of larger government and private sector organizations, their customers will be looking for the assurance that their small business partners are operating consistently with their own data protection policies and procedures.

What Small Businesses Can Do to Protect Themselves

Companies looking to strengthen information security practices should consider a three-prong risk management approach that uses a combination of policies, technology and people to address data protection. In the summer of 2003, the U.S. Federal Trade Commission held a two-part workshop on the current and potential role of technology in protecting consumer information. Workshop participants concluded that while technology can play a key role in protecting personal information, effective data protection requires a comprehensive approach that also addresses the critical roles that people and policies play in addition to technology.[5]

---

[3] http://wwwc.house.gov/smbiz/hearings/databaseDrivenHearingsSystem/displayTestimony.asp?hearingIdDateFormat=060316&testimonyId=483

[4] http://www.privacyrights.org/

[5] Federal Trade Commission Staff Workshop Report: Technologies for Protecting Personal Information, http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf

This holds true for small and large enterprises alike. In general, the complexity of information security increases with the size of the organization. In this sense, small businesses may have an advantage. However, small businesses do not have the same resources as large enterprises. For example, many small businesses cannot afford to hire experienced information security staff. As the FTC observed, security-enhancing technologies must be properly installed and maintained, and knowledgeable IT security professionals able to perform these functions today are in short supply.

Small business should begin by establishing a security policy. Several sources of guidance exist today, including the U.S. Chamber of Commerce's Common Sense Guide to Security for Small Business[6] as well as NCSA's tips. In addition, practical advice is available through the National Institute of Standard and Technology's SecureBiz workshops dedicated to small business.[7] These workshops are co-sponsorship with the Small Business Administration (SBA) and the Federal Bureau of Investigation (FBI), and they are especially designed for small businesses and not-for-profit organizations. Attendees have the opportunity to explore practical tools and techniques that can help them to assess, enhance, and maintain the security of their systems and information. Also under the Federal Information Security Management Act (FISMA), NIST has published several publications designed to assist with computer security, in particular its 500 and 800 series publications which are available on line.[8] This guidance was developed for Federal agencies, however the principles contained are applicable to small businesses. For example, NIST has issued guidance on categorizing systems based upon risk in order to help an entity more efficiently deploy scarce resources.

Steps the Information Security Industry is Taking to Improve Security

Improvements in technology have made basic security measures more available and affordable for small businesses. Systems are now being designed with security built-in, relieving end-users of the confusion and costliness of add-ons. Many security firms have developed products specifically designed for small businesses. A typical suite of security technologies includes: authentication, encryption, intrusion prevention, vulnerability testing, and monitoring technologies. Many of these capabilities are now bundled together or can be outsourced to managed security service providers. Other online services are available now free of charge to provide consumers with real-time advice on potentially dangerous sites which may contain spyware or generate unwanted e-mail. One example is a security add-on for web browsers called SiteAdvisor by McAfee. This service identifies web sites linked to spyware, adware, spam, viruses, browser-based attacks, phishing, or other online fraud. This free service has surveyed and tested 95% of the most frequently accessed web sites and notifies consumers of online "neighborhoods" that may pose more risk to their personal and financial information. Consistent with the FTC's principles and recent statements, technology such as McAfee SiteAdvisor has a role to play in protecting consumers online and can be applied without posing a heavy burden on owners of small businesses.

---

[6] U.S. Chamber of Commerce, Common Sense Guide to Security for Small Business, (September 2004); http://www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm
[7] National Institute of Standards and Technology, (http://csrc.nist.gov/securebiz/)
[8] NIST, see: http://csrc.nist.gov/publications/

The financial services industry, in particular the payment card industry, is seeking to improve information security among merchants through its Payment Card Industry (PCI) Data Security Standard. The PCI includes Visa, MasterCard International. They realize consumers must have confidence in conducting a secure electronic transaction from the point-of-sale. The PCI Data Security Standard, which went into effect last year, has 12 basic requirements that focus on using secure systems. The rules include installing a firewall, changing default passwords, protecting stored data, using antivirus software and encrypting transmissions of cardholder data across public networks. This top-down approach forces a common standard among merchants.

However, small businesses are beginning to face a new challenge in the growth of state legislation requiring the notification of consumers in the case of a breach of sensitive personal information. Some 29 states have passed data breach notification laws in 2005 and 2006 since California passed its law in 2003. The borderless nature of the Internet means that a small business must comply with all of the state laws. For example, if your business is based in Missouri and your database contains the name of California residents, you must notify those residents in case of a breach. While there is some similarity among the state laws, they set different thresholds for when a consumer must be notified, and the contents and means of notification vary from state to state. Local governments are also beginning to legislate in the area of security. Westchester County in New York has mandated security for wireless devices for business that deploy public Wi-Fi networks and required that they secure sensitive personal information.

The patchwork quilt of laws and regulations to address data security is beginning to look ugly. The laws and regulations place a burden on small businesses. There is an urgent need for Congress to pass legislation to create one standard by which all organizations will comply. Small businesses have limited legal and technical resources; therefore, they find the task of complying with different and potentially conflicting state statutes very difficult. Of all the segments of the business community, small businesses may have the greatest stake in the rapid adoption of a nationally pre-emptive data security law: any further delay by Congress leaves small businesses in an impossible legal situation. This is further complicated by the fact that small businesses must also contend with such laws as Sarbanes-Oxley. The SEC recently upheld that small businesses must comply with Sarbanes-Oxley despite intense pressure from various stakeholders.

Consumers too are also growing wary of the current situation, and are losing confidence in the information infrastructure. For example, CSIA's "Digital Confidence Index" showed a one point drop since December. The DCI is designed to measure the confidence of citizens in the security of the Internet. According to a survey CSIA commissioned in April by Pineda Consulting, half of the respondents avoided making purchases on line because of fear over identity theft or fraud. In addition, only 19 percent of respondents polled believe that existing laws are enough to protect their privacy.

Federal Government Action

There are several actions Congress and the Executive Branch can take to improve information security among small businesses, including passing a national data security law, greater leadership by the Small Business Administration and bolstering outreach efforts.

Implications of National Data Security Legislation for Small Businesses

As stated earlier, small businesses must enhance their data security capabilities in order to remain competitive with larger entities and to comply with existing state laws. The key is how to do so in ways that maximize protections without undue cost or burdens. One key answer is to enact a federal law that reflects this balance. CSIA believes that there are several provisions in pending legislation that are particularly important for small businesses:

Scope. Most state data breach laws apply to all organizations that hold sensitive personal data. Therefore, to ensure effective pre-emption, it is important that federal legislation apply to any agency or person who owns or licenses computerized data containing sensitive personal information; it should not be limited to "data brokers." Security breaches have occurred in a variety of industry sectors, and national legislation should be broader to include such groups and organizations as data brokers, banks, hospitals, educational institutions and large employers. This is important for small businesses because it assures consumers – the customers of small businesses – that their information will be protected regardless of where it is held or used. A more fragmented or limited approach will simply not enhance consumer confidence in doing business online.

Reasonable Security Practices. Legislation should set forth reasonable security measures based on widely-accepted industry standards, best practices or, where appropriate, existing Federal law, such as Gramm-Leach-Bliley (GLB) and the Fair Credit Reporting Act (FCRA). This is extremely important for small businesses because it sets forth a consistent, predictable national approach that gives clear guidance to small businesses that may otherwise struggle to determine on their own what reasonable standards are or how or when to apply them.

Notification Requirements. Small businesses will benefit from legislation that makes clear when notification is required, and that minimizes the need for notification when the likelihood of harm is low. In this context, a Federal law should include a "safe harbor" provision that would exempt companies from the obligation to notify in the event of a data breach when the data is encrypted. All state laws passed to date contain a similar provision. Such a provision may be useful to small businesses by encouraging the use of inexpensive and widely used methodology that can minimize costs associated with notification, lost reputation, and potential liability under the law.

Pre-emption. One strong federal law that pre-empts existing state laws would alleviate the compliance complexities small businesses currently face. As indicated earlier, this is a critical point and one we believe would make passage of a federal law attractive to small businesses.

Enforcement. Federal data security legislation does little to enhance consumer confidence absent strong and effective enforcement mechanisms. To this end, two specific provisions will be of particular importance to small businesses, as follows:

- **The Insider Threat.** The increasing threat presented by a malevolent or dissatisfied insider is an unfortunate reality for the entire business community, but for small businesses with limited detection and investigative resources, the implications can be particularly devastating. Legislation must ensure that provisions requiring reasonable security standards are enforceable so that consumers can be assured that actions by rogue employees or other insiders can be prosecuted. Inclusion of an enforcement requirement would bring data security legislation in line with other statutes (FISMA, HIPAA, GLBA) and provide a more uniform data protection regime.

- **Adequate resources for Federal enforcement.** The agency or agencies with enforcement authority should be granted adequate resources to properly and effectively enforce the law. This includes adequate funding, personnel, and tools to conduct thorough investigations, and prosecute and penalize offenders. The enforcing agency should also utilize existing standards wherever possible, rather than creating a new standard.

Executive Branch Leadership

Small business would benefit from more consistent leadership from the Federal government on the information security issues they face. Given the importance of IT as an enabler to small business, SBA should give information security far greater attention than it has to date. It should begin by establishing an office within the agency dedicated to the information assurance needs of small business, developing a comprehensive suite of programs. The SBA should also create an advisory committee comprised of small business community and technology leaders to advise the agency on programs specifically tuned to the challenges faced by small business.

Programs would be useful in several areas:

Information Assurance Survey. SBA should undertake a survey targeting small business to ascertain the specific challenges they face in securing networks. The Department of Homeland Security and Department of Justice have commissioned a survey targeted at larger businesses. Such a survey would provide for confidential results, but enable SBA to understand the types of attacks or disruptions small business are encountering and the associated costs. The results of the survey could inform SBA on key gaps requiring attention.

Tap InfraGard. SBA outreach should be expanded beyond SecureBiz. SBA should partner more consistently with InfraGard, a grass roots effort focused on critical infrastructure protection in tens of cities across the U.S. sponsored by the FBI. InfraGard brings together small and large business to share information and receive briefings on protection strategies. For example, InfraGard chapter members in San Francisco last week where briefed on the PCI Data Security Standard. The SBA need not create a new

network—one exists today. Within the context of InfraGard, SBA could sponsor regional or local information assurance small business awards recognizing innovation and leadership in information assurance.

NIST Guidance for Small Business. SBA should fund a NIST effort to publish guidance for small business. With appropriate funding, based upon guidance from an SBA advisory committee and the survey, NIST could publish information assurance guidance for small business.

Summary of Recommendations

CSIA offers the following recommendations for the Committee's consideration:

Create an Information Security Office within SBA. The office would serve as the Federal government's "go-to" organization for small business on information assurance. The office would act as a portal for receiving and dispensing educational information security tools and resources for small and medium-sized businesses. The office would chair the advisory committee, survey small businesses, and determine whether government programs and services are sufficient to serve the specific information assurance challenges they face.

Support national data security legislation. Small businesses have fewer resources and funding at their disposal to ensure they are in compliance with the laws of every state their businesses touch. A comprehensive, strong federal law will simplify the compliance process. Congress has introduced several bills, indicating its understanding of the importance of such legislation, and CSIA urges rapid enactment this year.

Take the message beyond the beltway. Reaching out to owners of small businesses on a local level is a more effective way to make known the resources and assistance available to small businesses. The NIST workshops I referenced earlier in addition to an expanded effort with InfraGard are examples of valuable local efforts. SBA leadership should draw from the existing network of programs already available to small businesses and conduct a broader outreach campaign.

A consistent approach to data security levels the playing field that is the online marketplace and enables small businesses to compete effectively for clients and customers with much larger businesses like no other time in the past.

I appreciate the opportunity to testify today, and I am pleased to answer any questions you may have.

U.S. HOUSE OF REPRESENTATIVES

Committee on Small Business
Subcommittee on Regulatory Reform and Oversight

Data Protection and the Consumer; Who Loses When Your Data Takes a Hike?

Testimony of

Lisa J. Sotto, Esq.
Partner
Chair, Privacy and Information Management Practice
Hunton & Williams LLP
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

May 23, 2006

Good morning. My name is Lisa Sotto and I am a partner in the New York office of the law firm of Hunton & Williams LLP. I head the firm's Privacy and Information Management Practice and also serve as Vice Chairperson of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee. Thank you for the opportunity to participate in this hearing. I am doing so on my own behalf and my views should not be attributed to Hunton & Williams, any client of the firm, or the DHS Data Privacy and Integrity Advisory Committee.

This morning, I will address three topics: (1) state security breach notification laws, (2) information security requirements applicable to U.S. businesses, and (3) my recommendations for a federal security breach notification law.

1. State Security Breach Notification Laws

In 2002, California enacted SB 1386, which became effective July 1, 2003. It is because of this law that we know about the many information security breaches that have occurred during the past several years. Essentially, the law requires organizations that own or license unencrypted, computerized personal information about California residents to notify those individuals if the security of their data was compromised.

Since the spate of publicized security breaches in 2005, 29 other states (in addition to California) have passed security breach notification laws. Similar legislation is pending in 11 other states.

While the various state breach notification laws are similar in many respects, they are not harmonized and contain some significant differences. For example, in 15 states, there is a harm threshold for notification. In Idaho, Kansas and New Jersey, an entity that suffers a data security breach is not required to notify individuals whose personal information may have been compromised if the entity determines that there has been no misuse of the information or that misuse is not reasonably likely to occur as a result of the breach. The trend in recently-enacted state breach laws is to include a harm threshold.

Another difference among state breach laws is in the definition of "personal information." Typically, "personal information" is defined in these laws as an individual's name *in combination with* Social Security Number; driver's license number or state ID card number; or account, credit or debit card number. Thus, if there is a security breach involving the unauthorized acquisition of "personal information" that could lead to identity theft, the entity that has suffered the breach must promptly notify affected individuals. In some states, however, the definition of "personal information" is broader. For example, in North Dakota, the definition includes date of birth and mother's maiden name, thus substantially broadening the notification requirement.

In addition, while most state breach laws cover only computerized data, North Carolina and Wisconsin also cover information maintained in hard copy format.

Some state breach laws contain additional notification requirements. For example, in Maine, New York, North Carolina and New Jersey, it is necessary to notify state agencies of a data breach. In numerous states, an affected entity also must notify consumer reporting agencies.

Needless to say, the variations in the 30 state security breach notification laws make compliance on a nationwide basis a complex matter.

2. Information Security Requirements Applicable to U.S. Businesses

I will now briefly outline the information security requirements applicable to businesses in the United States. First, the Gramm-Leach-Bliley Act's ("GLB") Safeguards Rule requires that financial institutions develop, implement and maintain a comprehensive, written information security program that contains administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer data. These safeguards should be appropriate to the size and complexity of the entity, the nature and scope of the entity's activities, and the sensitivity of the customer information the entity maintains. Entities that are subject to the Safeguards Rule also must (i) designate an employee to coordinate the entity's information security program, (ii) identify reasonably foreseeable risks to the security of customer information, and (iii) require service providers by contract to implement and maintain similar safeguards. In addition, every covered entity must continually evaluate and adjust its information security program in light of ongoing testing and monitoring of the system.

Another law that requires a formal, comprehensive information security program is the Health Information Portability and Accountability Act of 1996, known as HIPAA. HIPAA's Security Rule applies to electronic protected health information. Like GLB, HIPAA adopts a flexible and scalable approach to information security. The Security Rule states that "[c]overed entities may use any security measures that allow the covered entity to reasonably and appropriately implement the [required security] standards." In deciding which security measures to use, the covered entity must take into account (i) its size, complexity and capabilities, (ii) its technical infrastructure, hardware and software security capabilities, (iii) the cost of various security measures, and (iv) the probability and criticality of potential risks to its electronic protected health information.

A third information security requirement applicable to many U.S. businesses is found in California AB 1950 and its analogs in other states, such as Arkansas and Texas. AB 1950 requires businesses that own or license personal information about California residents to implement and maintain reasonable security procedures to protect the information from unauthorized access, destruction, use, modification or disclosure. The law also requires businesses that disclose personal information to nonaffiliated third parties to require by contract that those third parties maintain reasonable security procedures.

Pursuant to the Fair and Accurate Credit Transactions Act, the Federal Trade Commission ("FTC") promulgated a rule in 2004 that requires businesses to take reasonable steps to guard against unauthorized access to or use of consumer report information in connection with its disposal. In short, the Disposal Rule requires businesses to take steps to securely dispose of consumer report information. Several states have even broader data disposition laws. These laws generally require that, when a company is ready to dispose of records containing personal information, the company must take reasonable steps to destroy the records so they become unreadable or undecipherable. States that have such records disposition laws in place include Arkansas, California, Georgia, Texas and Wisconsin.

In addition, other laws may create security obligations indirectly. For example, the FTC has applied Section 5 of the Federal Trade Commission Act to sanction what it believes to be inadequate security as an "unfair" trade practice.

3. Recommendations for a Federal Information Security Law

Given the panoply of breach notification laws and information security requirements, I believe a federal law that would preempt similar state laws is critical. Because data often flows beyond state boundaries, a federal law would ensure that (i) personal information is subject to security requirements that are uniform throughout the nation and (ii) affected residents of every state would be notified of a data breach. Such a federal law should require businesses that collect and store sensitive consumer data to maintain reasonable security procedures to safeguard that data. This would provide consumers with uniform protection, regardless of where they live.

With respect to the breach notification requirements, I would advocate use of the California definition of "personal information" rather than an expanded definition adopted by some other states. The California definition is narrowly crafted to include only that information which is most commonly used by fraudsters to commit identity theft. Since the purpose of breach notification is to inform individuals of events that might cause them harm, there is no need to expand the definition to include data whose compromise would not subject an affected individual to identity theft or account fraud. In addition, I believe any federal law should contain a harm threshold. Notification should be required only if there is a real risk of harm resulting from a data breach. Finally, I would suggest that any federal law focus on computerized data rather than data maintained in another medium. Only information maintained in electronic format can be subject to the high volume of harm that these laws are specifically intended to combat.

I appreciate the opportunity to appear before you today to address these important issues. I would be glad to answer any questions you may have. Thank you.

Chairman Akin 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 information security.

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 information security and the incentives for small businesses to improve their information security practices. 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 Visa's 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 to card issuers. They also include card replacement costs, fraud monitoring costs, and incremental customer service costs. In order to protect its members from these costs, Visa aggressively protects the customer information of its members.

Typically, fraud losses are borne by the card issuer; however, rarely, if the merchant fails to follow proper authorization procedures for face-to-face transactions, costs may be passed back to the acquiring bank or the merchant that participated in the fraudulent transaction. For Internet, telephone and mail transactions, merchants are generally responsible for unauthorized purchases; however, Visa provides merchants with a number of tools to prevent fraud, and, by using Verified by Visa, merchants can shift these losses to the card issuing bank. Thus, even though some merchants may face potential liabilities associated with fraudulent card transactions, merchants are able to work together with Visa to substantially reduce the risk that the merchants themselves will suffer losses due to these transactions.

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 enterprises operating through brick-and-mortar stores, mail and telephone order centers or the Internet. CISP was developed to ensure that the customer information of Visa's members is kept protected and confidential. CISP

includes not only data security standards, but also provisions for monitoring compliance with CISP and sanctions for failure to comply. Visa has been able to integrate 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 new, common set of data security requirements, which is known as the Payment Card Industry Data Security Standard ("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 investigation and evaluation of the need for any card re-issuance.

In addition to CISP and the neural networks that monitor spending patterns, Visa has implemented a variety of 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 or 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 sales 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 is at an all-time low of five cents for every $100 worth of transactions.

In addition, Visa and the U.S. Chamber of Commerce have announced a new nationwide data security education campaign that will involve both the payments industry and merchants in the fight to protect cardholder information and reduce fraud. Visa

believes that all parties who 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 pending legislation in this area. In general, we favor federal legislation that would extend reasonable risk-based security and notification requirements to all entities that have sensitive customer information. We also believe that these policies 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 Thomas M. Lenard, Ph.D.
Senior Fellow and Senior Vice President for Research
The Progress & Freedom Foundation

Data Protection and the Consumer;
Who Loses When Your Data Takes a Hike?

Before the
Committee on Small Business
Subcommittee on Regulatory Reform and Oversight
United States House of Representatives

May 23, 2006

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Thomas Lenard and I am senior fellow and senior vice president for research at The Progress & Freedom Foundation. PFF's mission is to study public policy issues that affect the information economy, of which data security is surely one of the most important. Indeed, PFF recently held a day-long conference on the subject featuring FTC Chairman Deborah Majoras among others.

There are now about 30 states with data security laws and federal bills are moving through both houses of the Congress. These bills vary considerably in scope, but generally include some or all of the following:

- Requirements to establish a data security program with appropriate safeguards. These requirements may entail identification of an individual in the company responsible for the program; assessment of risks and vulnerabilities to data held by the firm; and development of

those vulnerabilities. Some bills include safe harbors for data encrypted using approved methods.

- Requirements for notification of affected individuals in the event of a security breach. Depending on the circumstances, notification may be by mail, email, or through the company's web site or the mass media. Along with the notification requirement, companies may be required to provide credit reports to the victims of a security breach.
- Provisions that affect the collection and commercial use of personal information generally. These include restrictions on the use of identifiers, such as Social Security numbers, as well as special requirements for data brokers, including establishing procedures for audits and consumer access to their information.
- Federal preemption of state requirements.

In order to decide whether regulations such as these are desirable, and, if so, in what form, the following basic public policy questions need to be addressed:

- Are there "failures" in the market for data security?
- If market failures exist, how do they adversely affect consumers?
- Can such failures be remedied by government action?
- Would the benefits of government regulation exceed the costs?

An Illustration: The Benefits and Costs of Notification Requirements

To illustrate the benefit-cost approach to these issues, I'd like to summarize an economic analysis of notification requirements for data security breaches I recently did with Paul Rubin, who is a professor of law and economics at Emory University as well as an adjunct PFF fellow. That study is attached to my testimony.

Our study addresses a number of interrelated issues concerning whether a notification requirement would be in the best interests of consumers and what form it should take:

- Does the private market provide adequate incentives for firms both to secure their data and to provide notice to consumers in the event of a breach?
- Is there reason to believe a notification requirement will yield benefits greater than costs?
- In light of the benefit-cost analysis, how should a notification mandate be structured?
- If there is a requirement, should it be at the state level or should federal law preempt state laws in this area?

The major conclusions of the study are:

- The annual costs of identity theft and related frauds are $55 billion, $50 billion of which are borne directly by businesses, including banks, credit card issuers and merchants. Firms also suffer large losses in stock value when security is breached. These factors provide strong incentives for companies to spend money on data security.
- It is unclear whether firms also have adequate incentives to notify compromised consumers, so the issue is an empirical one: do the benefits of notification outweigh the costs?
- The expected benefits to consumers of a notification requirement are extremely small—on the order of $7.50 to $10 per individual whose data have been compromised. This is because (1) most cases of identity theft do not involve an online security breach; (2) only a very small percentage of individuals compromised by security breaches—perhaps 2 percent—actually become victims of a fraud; (3) most of these are victims of fraudulent charges on their existing credit accounts, for which they have very limited liability, rather than victims of true identity theft; and, (4) even a well-designed notification program will only eliminate about 10-20 percent of the expected costs.
- The direct costs of notification may be less than $10 per individual (our estimate of the maximum benefit), but only for relatively large notification programs. This is at least in part because most data security statutes

permit alternative, less expensive methods (e.g., email or posting on a website) once a dollar or number-of-victims threshold is reached.

- However, the major regulatory costs to be concerned about are not the direct costs of notification. Rather, they are the costs incurred when consumers and firms overreact and take actions that are harmful to themselves and to the free flow of information. Consumers, for example, may be induced to place fraud alerts on their accounts or close them entirely, actions that are likely to be far more costly than being an identity theft victim. They may also be induced to shift their credit transactions offline, which the data show would actually increase their exposure to identity theft.
- Because a notification mandate is dubious on benefit-cost grounds, it should be targeted carefully. Firms should be able to determine which customers are most at risk and tailor notice to those individuals, perhaps in cooperation with the FTC.
- Federal preemption of state notification laws will reduce compliance costs and improve the benefit-cost balance. A true federalist approach is not possible with markets and firms that are national, and even international, in scope. Firms will tend to comply with a single set of rules. In the absence of a preemptive federal statute, they will comply with the most stringent set of state regulations, which will in effect "preempt" other state regulations.

Effect on Small Business

The effect of data security regulations on small businesses should be an important part of the benefit-cost calculus. These regulations impose a per unit burden that is inversely related to the size of the company, which means that it is less likely that a notification requirement applied to small firms will pass a benefit-cost test than would be the case for large firms. In addition, the added costs could have an adverse effect on competition, because they make it more difficult for firms to enter markets in which the use of personal information is important.

There are a number of ways in which data security regulation disproportionately affects small firms and I'll give a few examples.

First, the requirement to establish a data security program involves costs that are largely fixed. For example, establishing such a program entails retaining specialized expertise, including computer, data management and legal expertise, either in-house or from outside. These costs are likely to be relatively invariant with the size of the firm and therefore higher per unit of output for small than for large firms. Many of the costs are also what economists call "sunk" costs, which means they are not recoverable if, for example, the business fails. This is an added burden that will deter start-ups and could have an adverse effect on competition.

Second, establishing a safe harbor for companies that encrypt their data is also likely to disfavor small businesses. Encryption is often quite expensive and its costs are not sensitive to firm size.

Third, many of the costs of a notification program, including assessing the risks associated with a breach, and designing the notice and the rest of the program, are also likely to be relatively fixed and therefore to decline on a per unit basis with the number of individuals being notified and the size of the business. Costs of some of methods of notification—e.g., posting a notice on the company's web site and using the mass media, may be totally invariant with respect to the size of a breach. This bias against small businesses is exacerbated by provisions that allow "alternative notice" if individual notice exceeds a trigger—either in terms of number of individuals or cost. Thus, depending on how the statute is worded, a large company suffering a large breach may not be required to undertake individual notice while a small company may be required to do so because it doesn't trigger the alternative notice requirements.

Fourth, without federal preemption, companies are faced with the prospect of familiarizing themselves with numerous different state laws to make sure they are in compliance. The costs associated with this, which also do not vary much with firm size, constitute a particular burden for smaller firms. Federal preemption, if enacted, will eliminate these costs and work to the advantage of small firms.

Finally, it is important to note that any regulation of the information sector that raises the costs of targeted advertising and obtaining accurate customer lists has a greater adverse effect on new entrants and small firms than it does on large, established firms. This is particularly true for Internet advertising, where established firms have lists of their own customers and visitors to their web sites, but new firms must purchase such lists. As long as there is a market for customer lists and other such information, entrants can begin competing relatively easily. However, if regulation should reduce the size of the market and increase costs, competition from new entrants would be reduced.

All of this does not imply that data security regulations are necessarily a bad thing. But, it does point up the need to subject them to rigorous benefit-cost analysis to assure that, if adopted, their benefits are sufficient to justify their costs.

THE PROGRESS & FREEDOM FOUNDATION

Progress on Point

Release 12.12 July 2005 Periodic Commentaries on the Policy Debate

AN ECONOMIC ANALYSIS OF NOTIFICATION REQUIREMENTS FOR DATA SECURITY BREACHES

By Thomas M. Lenard and Paul H. Rubin*

I. INTRODUCTION AND SUMMARY

Congress and the states are moving rapidly to enact new legislation in the wake of a series of high-profile data security breaches by both private and public institutions.[1] Bills have been introduced that would impose a variety of obligations on both businesses and public-sector entities in the event of a security breach, and provide remedies for individuals whose personal information was acquired by an unauthorized party. A major component of all the legislative proposals is a requirement that consumers be notified when a security breach occurs that might compromise their confidential data.

In 2003, California became the first state in the nation to enact a security breach statute.[2] Indeed, the California notification requirement was responsible for the initial publicity surrounding a security breach by information broker ChoicePoint, and the subsequent demand for further legislation. At the present time, thirteen states have security breach legislation in place.

Press accounts and statements from various experts give the impression that identity theft and related frauds are on the rise (Fountain, 2005). For example, the preamble to the California security breach statute states that "[i]dentity theft is one of the fastest growing crimes committed in California." But while identity theft is clearly a major problem, the data do not show that it has been increasing over time.

The most comprehensive data on identity theft and its costs are from a survey commissioned by the Federal Trade Commission and carried out by Synovate in 2003. This analysis was updated for 2004 by Javelin (2005). Virtually all the results, including incidence of identity theft and costs to victims, are about the same (not statistically

---

* Thomas Lenard is senior fellow and vice president for research at The Progress & Freedom Foundation. Paul Rubin is Samuel Candler Dobbs Professor of Law and Economics at Emory University and adjunct fellow at PFF. This paper reflects the views of the authors and not their respective institutions.

[1] In addition to the ChoicePoint security breach, there have been major security breaches involving DSW Shoe Warehouse, Boston College and several other universities, Polo Ralph Lauren, Ameritrade and CardSystems.

[2] Bill Number 700, available at http://www.leginfo.ca.gov/pub/01-02/bill/asm/ab_0651-0700/ab_700_bill_20020929_chaptered.html

different) in the two surveys, indicating that fears of identity theft being a rapidly growing problem are exaggerated.[3]

The Synovate and Javelin surveys show that the costs of identity theft and related crimes were essentially constant over the last two years for which data are available. Other data suggest these costs have been decreasing over time. Estimates by Nilson show the total costs of credit card fraud to issuers decreased from $882 million in 2003 to $788 million in 2004—a 10-percent decline (Nilson Report, 2005). Moreover, over a longer period—1992 to 2004—the Nilson Report found that the costs of these frauds have decreased, from $0.157 to $0.047 per $100 in credit card sales.[4] This is not surprising, despite the press accounts, because credit card firms are continually updating and improving levels of security (Bank and Clark, 2005; Pacelle, 2005). The Nilson Report also indicates that fraudulent charges are lower as a percentage of credit card use in the U.S. than in the rest of the world; for example, credit card payments in the U.S. are three times the U.K. level, as compared with fraudulent charges, which are only about 1.2 times the U.K. level.

This paper addresses a number of interrelated issues concerning whether a notification requirement would be in the best interests of consumers and what form it should take:

- Does the private market provide adequate incentives for firms both to secure their data and to provide notice to consumers in the event of a breach?
- Is there reason to believe a notification requirement will yield benefits greater than costs?
- In light of the benefit-cost analysis, how should a notification mandate be structured?
- If there is a requirement, should it be at the state level or should federal law preempt state laws in this area?

Our major conclusions are:

- The annual costs of identity theft and related frauds are $55 billion, $50 billion of which are borne directly by businesses, including banks, credit card issuers and merchants. Firms also suffer large losses in stock value when security is breached. These factors provide strong incentives for companies to spend money on data security.

[3] The actual incidence of identity theft of all forms decreased from 4.7 percent of the adult population to 4.25 percent, but this difference was not statistically significant.
[4] This represents costs to card issuers, and so is not comparable to the FTC numbers, which represent total costs to all businesses and consumers.

- While it is unclear whether firms have adequate incentives to notify compromised consumers, the issue is an empirical one: do the benefits of notification outweigh the costs?

- The expected benefits to consumers of a notification requirement are extremely small—on the order of $7.50 to $10 per individual whose data have been compromised. This is because (1) most cases of identity theft do not involve an online security breach; (2) only a very small percentage of individuals compromised by security breaches—perhaps 2 percent—actually become victims of a fraud; (3) most of these are victims of fraudulent charges on their existing credit accounts, for which they have very limited liability, rather than victims of true identity theft; and, (4) even a well-designed notification program will only eliminate about 10-20 percent of the expected costs.

- Because a notification mandate is dubious on benefit-cost grounds, it should be targeted carefully. Firms should be able to determine which customers are most at risk and tailor notice to those individuals, perhaps in cooperation with the FTC. Encrypted data should be exempt from notice, because it is less likely to be used for fraudulent purposes.

- Federal preemption of state notification laws will reduce compliance costs and improve the benefit-cost balance. A true federalist approach is not possible with markets and firms that are national, and even international, in scope. Firms will tend to comply with a single set of rules. In the absence of a preemptive federal statute, they will comply with the most stringent set of state regulations, which will in effect "preempt" other state regulations.

II. THE COSTS OF SECURITY BREACHES

The FTC estimates that ten million people—or about 4.6 percent of the adult population—are victims of some form of identity theft annually. The estimated out-of-pocket costs of this identity theft are about $55 billion annually, of which about $50 billion are borne by businesses and $5 billion by consumers.

There are two categories of identity theft. Misuse of an existing credit card or other account—i.e., charging items on someone else's account—accounts for two thirds of the total number of incidents. The remaining third consists of opening up new accounts in another person's name and related frauds. This latter category—which corresponds more closely to true identity theft—is substantially more costly to both businesses and individuals. Victims of this type of identity theft incur substantial monetary and time costs attempting to clear up their damaged credit records. In this paper, we follow the convention of including both types of fraud under the rubric of identity theft.

Estimates of the costs of identify theft based on the FTC data are summarized in Table 1. The FTC estimates the average cost to business of new and existing account

fraud is $10,200 and $2,100, respectively. The weighted average cost of an incident is about $4,800.

Table 1: Costs of Identity Theft			
	New Account Fraud	Existing Account Fraud	Total
Incidence (last year)	1.5%	3.1%	4.6%
Weight	0.326	0.674	1.00
Cost to businesses	$10,200	$2,100	$4,800*
Cost to Individuals	$1,180	$160	$500*
Time spent by individuals	60 hrs.	15 hrs.	30 hrs.*
Cost of time @ $15 per hour	$900	$225	$450*
Total cost to individuals	$2,080	$385	$950*

* Weighted averages of new and existing account fraud (totals are rounded).
Source: Computed from Federal Trade Commission (2005), Identity Theft Survey Report, Synovate, September, available on the FTC website.

The cost to individuals of a new account fraud is $1,180 and 60 hours of time. Using $15 per hour as the average wage rate (value of time) (Bureau of Labor Statistics, 2005), this yields a time cost of $900 and a total cost of $2,080. A similar calculation for existing account fraud yields a total cost per incident of $385. The weighted average cost for all types of incidents is $950. Since the incidence of all forms of identity theft is 4.6 percent, the expected cost to the average consumer is about $50. As discussed below, however, any notification requirement will save consumers considerably less than this amount.

III. MARKET RESPONSES

A. Security

As just discussed, the FTC study found that the costs to businesses of identity theft are about 10 times the costs to individuals. The prospect of reducing a $50-billion loss means that the businesses involved—the credit card companies, the banks, merchants and others—should have a strong incentive to invest in data security.

These costs are reflected in the large stock market losses suffered by firms victimized by security breaches. Garg et al (2003) found that firms victimized by a security breach involving theft of credit card information suffered a stock market loss of 9.3 percent on the first day the breach was announced, increasing to 14.9 percent over

three days. This cost is quite large—three to five times the amount found in similar studies for other classes of events.[5] Most breaches involving other types of data did not exhibit significant stock market effects. Similarly, Campbell et al. (2003) found that there was no significant effect of breaches that did not involve data security, but that breaches associated with violations "such as customer databases" did lead to significant losses in stock value. It is important to note that these results are from a period before any consumer notification was required. Nonetheless, information about the breach became public—perhaps as a result of securities regulatory requirements—and markets reacted accordingly. Thus, even without any laws mandating notice to consumers, firms have had a very strong incentive to avoid data security breaches because the market penalizes them severely.

This is reflected in the behavior of the credit card companies, which continue to devise new and better security systems as they compete to sign up merchants (Bank and Clark, 2005; Pacelle, 2005; Morriss and Korosec, 2005). While the primary purpose of increasing security is to reduce the costs of fraud to businesses, the costs to consumers are also reduced. The guarantee that consumers are liable for no more than $50 (and often for nothing) if a credit card is misused is essentially a form of insurance provided by issuers and merchants to credit card holders. In a competitive economy, the costs of this insurance are ultimately passed on to consumers in the form of higher prices for goods and services. Thus, the expenditures that businesses make to enhance security (and reduce the costs of fraud) will produce benefits in the form of lower prices for consumers.

Because some of the costs of fraud (around 10 percent) are borne by consumers and thus are external to the firm, the level of security might be suboptimal,[6] but only very slightly so. The level of security would be "almost optimal" since firms bear almost all of the costs directly.

B. Notification

Security and notification are two different things. While the incentives to provide security may be close to optimal, the same may not necessarily be the case for notification. The major incentive a firm or other information holding entity would have to inform consumers of the loss of data is reputational. That is, credit card issuers or others might try to use notification as a dimension of competition—for example, claiming that "we always inform you if your information is lost." If consumers value this commitment, the market would sort itself out so that those firms not promising notification would be at a competitive disadvantage.

---

[5] For example, the cost of FTC advertising cases is 3-6 percent (Peltzman, 1981); the cost of Food and Drug Administration recalss is 5.6 percent (Jarrell and Peltzman, 1985); and the cost of Consumer Product Safety Commission recalls is 5.4-6.0 percent (Rubin et al., 1988).

[6] That is, firms would equate private marginal costs with private marginal benefits, but social benefits of security would be higher than private benefits because firms bear only 90 percent of the costs of security braches.

There are, however, several reasons to think that this mechanism might not be adequate. Most importantly, information can be lost by many entities with no direct connection to consumers. For example ChoicePoint itself has no connection to consumers, and so would not be in a position to commit to notification. Similarly, a recent incident involved information loss by CardSystems, a previously little-known firm that processes information for credit card companies but has no connection to the card holders themselves (Dash and Zeller, 2005). Moreover, information is held and sometimes lost by firms which do not appear to be in the information business, such as retailers and universities. Such entities would not advertise information policies, and consumers would not expect them to. For example, between February and April 2005 information was lost by entities as diverse as DSW Shoe Warehouse, Boston College, Polo Ralph Lauren and Ameritrade (Wall Street Journal Online, 2005). Moreover, because of various complexities in the processing of credit card transactions, in most cases a consumer will not really know who is processing his transaction or what rules are being used (Morriss and Korosed, 2005).[7]

In addition, characteristics of the credit card industry might adversely affect incentives for notice. Consumers are liable for at most $50 of the value of any goods or services purchased using their cards fraudulently, and in most cases even this is waived. But they must notify the card issuer of the fraud to avoid such charges. The costs are then generally borne by the merchant if a card is used fraudulently, or the issuing bank when a counterfeit card is used (Morriss and Korosec, 2005). Thus, a merchant might not have an incentive to inform a consumer of a fraudulent use because this would then cost the merchant money.

Nonetheless, it is possible that the major credit card companies (Visa, MasterCard, American Express, Discover) would require such notice for competitive reasons. These entities are sufficiently central in the contracting process that such a requirement could be enforced on all parties involved, whether the parties have a direct relationship with consumers or not.

In sum, it is unclear whether the market incentives for customer notification are adequate or not. Whether or not a regulatory notification requirement will be welfare enhancing is then an empirical question: are the expected benefits greater than the expected costs?

IV. BENEFITS OF NOTIFICATION

The benefits of a notification requirement consist of the reduction in the costs associated with identity theft. We derive a benefits estimate two ways, both of which give essentially the same result. The first estimate uses the average cost of identity theft (see Table 1) for the population as a whole as a starting point and then estimates the maximum portion of that cost that might conceivably be reduced by a notification requirement. The second estimate uses an independent estimate of the probability that

[7] There are several parties involved in any transaction, including the credit card company, the bank issuing the card, and various intermediate processors, such as CardSystems.

a compromised card will be used fraudulently as the starting point. After adjusting both estimates for the effects of delay in notification, we conclude that the potential benefits of notification are on the order of $7.50 to $10 per individual whose personal information has been compromised. There is some reason to believe that even these estimates are too high.

A. Estimate 1

The expected cost per person of identity theft, based on the FTC data, is $50. This provides an upper bound for the potential benefits of any new regulatory requirement.

Javelin (2005) estimates that only 11.6 percent of the cases for which the source of the security breach is known involve an online source. Sixty-eight percent of these cases involve an offline source—for example, a lost or stolen credit card, or a relative, friend or neighbor having access to credit card bills. The remaining 20 percent presumably involved cases where it is not known whether the source was online or offline.

Notification only affects online security breaches. If we assume that all of the cases not explicitly identified to be offline are in fact online—a very conservative assumption—then only about 30 percent of the costs of identity theft could possibly be ameliorated by notification. This would reduce the maximum potential benefits to $15 per consumer.

Although we use this estimate, it is clearly still too high for several reasons. For one thing, it assumes that all breaches not explicitly identified as offline are online, when, in fact, a substantial fraction of the source-unknown thefts (perhaps the same fraction as those for which the source is known) are also offline.

In addition, notification only affects data stolen from businesses. Many online thefts do not involve businesses. Many occur, for example, when consumers are tricked into providing passwords to accounts (Pegoraro, 2005). According to one expert such theft represents "what most attackers seem to employ these days." One estimate is that about one million consumers were victims of this tactic, known as "phishing" (Pacelle, 2005).

The FTC survey indicates only 6 percent of the identity theft cases where the thief is known involve an employee of a firm.[8] In 15 percent of those cases the thief is a relative, friend or neighbor. In 14 percent, the problem is a lost or stolen card. These data suggest that only a subset of online breaches involve businesses that would be affected by a notification requirement.

[8] The FTC study found that the thief was known in 50 percent of the cases.

B. Estimate 2

This estimate is based on an estimate attributed to Visa that 2 percent of compromised cards are used fraudulently.[9] This number also represents the probability that a compromised consumer will actually be a victim. Using the estimated consumer cost per incident of $1,000, this means that the expected cost to a person whose identity is compromised—and, therefore, the maximum benefit of notice—is $20.

The Visa 2-percent probability estimate is roughly consistent with other indirect evidence from this market. For example, some experts estimate that it does not pay for issuers to issue new cards, at a cost of between $10 and $20, for compromised accounts (Sidel and Pacelle, 2005). This cost, combined with the estimated $2,000 cost to business of an actual incident involving misuse of an existing card (see Table 1), suggests that, if it doesn't pay issuers to issue new cards, then the probability of a compromised card actually being misused must be no more than 1 percent, slightly lower than Visa's 2-percent estimate.[10]

Evidence from underground markets that use websites to trade stolen information is also consistent with this probability estimate (Bryan-Low, 2005; Zeller, 2005). Information enabling the use of stolen cards sells for between $50 and $200 per card on such websites. Another price quoted is 5 percent of available credit. These values imply that many cards are not used, or not used intensively. If the average amount stolen from a business is $2,000 and a card sells for $200, this implies that there is only a 10-percent chance of the card actually being used; a $50 price implies a 2.5-percent chance. One gang that was recently arrested ("Shadowcrew") apparently sold two million credit card account numbers and caused over $4 million in losses to financial institutions and others. If the average loss caused was $2,000, this suggests that there were 2,000 transactions involving the two million stolen cards—a rate of 0.1 percent, significantly lower than the Visa estimate.

The news media began reporting intensely on identity theft after the ChoicePoint incident, which involved about 145,000 individuals. This was reported to the public on February 15, 2005. As of April 20, there were 750 known cases of fraud involving these individuals (Wall Street Journal Online, 2005). This is an incidence of 0.5 percent in a two-month period. If this rate continues for the entire year, then 3 percent of the compromised persons will be victimized, slightly higher than Visa's 2-percent estimate.

In another incident, 310,000 persons were at risk from an incident involving LexisNexis on March 9. Of these, 59 cases of illegal action were known as of April 20. This represents a trivial fraction, but there may have not been enough time for victims to

---

[9] This estimate is widely reported in the press (see, for example, Sidel and Pacelle, 2005). It also has been confirmed in discussions with representatives of Visa.

[10] An issuer would be indifferent if the cost of the new card, say $20 was equal to the expected loss (the probability of a fraud times $2000). The probability level at which the issuer would be indifferent is 1 percent [$20 = (0.01) x ($2000)]. It would not pay for the issuer to issue a new card if the probability was less than 1 percent.

be identified in the month between the initial report of the incident (March 9) and the compilation in the Wall Street Journal (April 20).

C. Reduced Benefits Due to Delay

Providing notice to consumers takes time. A firm must first learn of the identity theft, and, while it is doing so, the thieves can be using the stolen data. Second, a firm must determine whose identities have been stolen, often by recreating the data. This is time consuming. Third, the California law and almost all other laws, whether enacted or proposed, allow the firm to delay notice if it is cooperating with a law enforcement agency. This also delays the ability of the firm to provide notice. For example, in a recent well-publicized case involving 40 million records, MasterCard observed some atypical levels of fraud in mid-April 2005, but did not provide any notice until mid-June.[11] Moreover, the FBI is still investigating the matter, so that further delay would have been possible (Dash and Zeller, 2005). Thus, in the best of circumstances, notification means that consumers might be able to respond more quickly to identity theft, not to avoid it altogether.

The FTC data provide some insight into the time profile of identity theft losses. For those consumers who discovered identity theft within five months, 67 percent had no out of pocket expenses. For those who did not discover the theft for six months or more, only 40 percent had no out of pocket costs. For those who discovered the theft within one month, 76 percent were able to resolve their problems in less than 10 hours, while for those who discovered the theft after more than six months only 20 percent were able to accomplish this in less than 10 hours. These data are difficult to extrapolate, but they suggest that normal notification delays can have a significant effect on losses, if active identity thieves are involved. We assume this factor reduces the benefits of notice by 50 percent. This reduces the benefits to about $7.50 to $10.

D. Consumer Response

Even when consumers receive notice of a security breach, many of them do nothing about it. For most people, this is probably the best response, because most compromised data are not misused and "doing something about it" is far from costless. The FTC survey indicates that even among those who have been victims of identity theft, 55 percent indicate that they are "not very" or "not at all" concerned that they will be victimized again. Thirty-eight percent of victims reported to no one, including even the credit grantor or place of misuse. The FTC indicates that only 26 percent of actual victims reported to the police and only 22 percent of victims reported to credit bureaus; of these, 62 percent asked for a "fraud alert." In other words, only 14 percent of actual victims asked for a fraud alert. Thus, if only a small percentage of actual victims make use of alerts, it is unlikely that many persons who only were notified of a breach will do so, because the probability of actual ID theft is still very small.

[11] It is not clear that the notice provided by MasterCard was consistent with the requirements of the various state laws.

As indicated above, the evidence suggests that only about 2 percent of those who are exposed are actually victimized. In addition, for most forms of victimization, the costs are minimal; credit cards guarantee that consumers pay a maximum of $50 of any loss. Finally, in many cases, the costs (in inconvenience) of taking action may be as great or greater than the costs of being victimized—and the costs of taking action are certain, while the costs of victimization are only probabilistic and are only incurred in the unlikely event that one is actually a victim.

The fact that most consumers do not take any action when notified further reduces the benefits of notice. Nonetheless, we do not adjust for this factor since there is no current way to measure the probability that a compromised individual will actually take any action. Thus, the benefit estimate of $7.50 to $10 may be biased upwards. Any actual benefit will likely be less than that amount.

V. COSTS OF NOTIFICATION

There are three categories of potential costs associated with a notification requirement: the direct notification costs; the costs of actions taken by consumers as a result of notification; and the costs in terms of a diminished flow of information resulting from actions that firms might take in response to a publicized security breach.

A. Direct Notification Costs

The California statute requires written or electronic notice, but it allows "substitute notice" if the "cost of providing notice would exceed two hundred fifty thousand dollars or the affected class or subject persons to be notified exceeds 500,000." "Substitute notice" includes emails, posting on a website, and notification of major statewide media. Other state bills, proposed and enacted, seem to have adopted a similar approach. This would place the maximum cost of notification at $250,000.[12] Given that the upper bound estimate of the benefit of notice seems to be no more than $10 per person (as discussed above), any breach involving more than 25,000 victims might justify the cost of notice.[13] The cost of writing a letter has been estimated at $2 per person (Sidel and Pacell, 2005), which would imply that notice might barely be worthwhile if this was the only cost. However, there are additional costs that are more important.

B. Costs of Actions Taken by Consumers

Costs to consumers as a result of actions they take may be more significant than the direct costs to firms of providing notice. The FTC (FTC, n.d.) and others recommend the following actions for those who are or suspect they are the victims of identity theft: Place a fraud alert on your accounts and close the accounts "that you know, or believe" have been tampered with fraudulently. A fraud alert means that a

[12] As shown below, the cost might be much greater because of the lack of coordination between states.
[13] This discussion does not take into account the fact that there is likely to be some variation in the effectiveness—and therefore the expected benefits—associated with the different methods of notification. Otherwise, there would be no point in not permitting the least-expensive methods to begin with.

business must verify the consumer's identity before issuing credit, generally by contacting the consumer directly before issuing credit. The FTC indicates that "[t]his may cause some delays if you're trying to obtain credit." In many circumstances, the agency also recommends closing accounts, which may be even more costly, particularly if consumers have set up accounts to automatically pay recurring bills.

All these costs are likely to be significantly greater than the expected costs of compromised individuals actually being victimized. Recall that we estimated these costs to be about $20. This explains why it is perfectly rational for most consumers to do nothing, even when notified that their data have been compromised.

Additionally, consumers can impose costs on firms. A consumer notified about some threat may request a new card. The cost of issuing a new card is estimated at between $10 and $20, which is about equal to the expected cost (to the consumer) of actually being a victim.

There is an even more significant potential cost, which is difficult to quantify. As consumers start to receive more notices, they may become increasingly afraid to do business online (Fountain, 2005). This would be a costly reaction, because, as the Javelin Report shows, online commerce is safer than traditional offline commerce. For example (p. 7): "the current data on the source of access clearly evidences that consumers are most at risk when using traditional methods." A second finding (p. 10) is that "[t]he single most effective approach to protect against both external and domestic identity theft is to turn off all paper bills and statements." The Javelin Report also indicates (p. 4) that the mean time for fraud detection for paper statement review is 114 days, with a mean cost of $4,543; the comparable numbers for electronic accounts are 18 days and $551. It is quite plausible that a continual stream of warnings could lead consumers to decide that online commerce is riskier than traditional offline paper commerce and, consequently, shift away from the online mode. This would have the effect of increasing the identity-theft risks to which they are exposed.

C. Information Costs

As discussed above, if a firm provides notice of loss of data under its control, it will suffer a loss of reputation and share value. From society's point of view, however, the threat of a loss of reputation may be a good thing, stimulating firms to provide better security for their data. Thus, the private cost to the firm may be socially beneficial.

Firms may, however, overreact in an effort to minimize the costs associated with loss of reputation. We know that the information provided by firms in the information market is of great value to consumers and the economy (Rubin and Lenard, 2002). Any reaction that reduces the value of this information can easily outweigh any benefits of notice. For example, as a result of a reaction to the loss of information on 300,000 individuals, LexisNexis began restricting access to Social Security and drivers' license numbers to a limited class of users (New York Times, 2005). ChoicePoint has also begun restricting use and provision of its information in many ways (Solove and

Hoofnagle, 2005). One fallout from these policies is that it will be more difficult for new firms to enter some markets, because it will be more difficult for them to obtain the necessary customer data. It is likely that the net effect of these and similar policies will be to reduce consumer welfare.

VI. ARE THE BENEFITS OF NOTIFICATION GREATER THAN THE COSTS?

The expected benefits to consumers of mandatory notification are only about $7.50 to $10 per individual whose personal data has been compromised due to a security breach. This is obviously an extremely small number.

There are several reasons that the expected benefits are so small: First, most cases of identity theft involve offline security breaches, which are not affected by notification. Second, the probability of an individual compromised by an online security breach becoming an identity theft victim is extremely small. Third, most of those victims don't really have their identity stolen. Instead, the fraud consists of charging items to the victims' accounts—charges for which the account holders have very limited liability. Finally, even a well-designed notification program is likely only to eliminate a small fraction of the expected costs—we estimate about 10 to 20 percent.

Given these very small expected benefits, it is difficult for a notification mandate to pass a benefit-cost test. While the direct costs to notifying firms may not be large, the indirect costs both to consumers and to sectors of the economy that depend on the free flow of information are likely to be substantial, primarily because of the likelihood that both consumers and firms suffering a security breach will overreact to notification. Of particular concern is the fact that consumers would increase their risk exposure if they shifted from online to paper-based transactions as a result of the publicity associated with multiple notifications.

Finally, this all should be put in the context of the trend data, which indicate that the true risk of identity theft and related frauds is not increasing and may actually be decreasing over time. Thus, the market incentives seem to be alleviating the problem and it is likely that consumers' perceptions of the risks—which perhaps currently are exaggerated—will adjust accordingly.

VII. OPTIMAL SCOPE OF NOTICE

The discussion above suggests that any notification requirement is dubious on benefit-cost grounds. Thus, any new statute that is passed should be carefully targeted to individuals most at risk.

There are several dimensions on which mandated disclosures could be targeted. One is encryption. The California law deals only with unencrypted data, and this is a useful limitation. Since only a small percentage of compromised records are actually misused, it is very unlikely that encrypted records are among them.

A second issue concerns the population to be notified (Pacelle and Conkey, 2005). In situations where the firm has good reason to believe that only a fraction of the potentially compromised consumers are at risk, the notice should be tailored to those consumers. In addition to the direct expense, an overly broad notification requirement might cause consumers to become inured to receiving such notices or to withdraw needlessly from various forms of commerce due to excessive fear of identity theft (Fountain, 2005.) This is especially dangerous since, as mentioned above, online commerce is actually safer than offline commerce.

VIII. THE ISSUE OF PREEMPTION

Thus far, security breach legislation has been introduced in at least 35 states and adopted in at least 13 states: Arkansas, California, Connecticut, Florida, Georgia, Illinois, Indiana, Maine, Minnesota, Montana, North Dakota, Texas and Washington. Bills are now sitting on the governor's desk in Nevada and Tennessee. The question is whether it would be better to allow each state to approach this issue as it sees fit or to have a federal law that preempts state laws and subjects the whole country to the same set of rules.

A. Benefits of Federalism

As a general matter, there are two major benefits to a federalist approach. The preferences of individuals may not be the same everywhere and it is better if states are able to adopt rules tailored to the preferences of citizens. In addition, a federalist approach makes it possible to experiment with different rules at the state level (the states can be laboratories) and this can reduce the risks associated with adopting a single set of rules at the federal level that may be flawed in ways that we don't foresee.

It is questionable, however, whether true federalism is possible for firms operating in a market that is (at a minimum) national in scope. For these companies, information breaches don't just affect citizens in one state. When a breach occurs, virtually any firm that operates in a number of states will apply the same notification policy to everyone affected.

The California law went into effect in 2003, but the major event drawing attention to the issue was the ChoicePoint incident in early 2005. Initially ChoicePoint planned to disclose the breach only to California residents, as required by law. However, once the breach was publicized, pressure quickly mounted to make the same disclosure to everyone who was affected. Since then, most (if not all) firms suffering breaches have followed the same policy and disclosed to everyone. If this is the general practice, then it appears that the most stringent state law or set of provisions taken from various state laws (in the sense of requiring disclosure to the largest number of people in the largest set of circumstances) will govern all states. We would not have the benefits of a federalist approach even if the federal government does not formally preempt state laws. Rather, there will be implicit "preemption" by the most regulatory state or states.

This also applies to the levels of data security that firms maintain, which are closely related to disclosure requirements and are often part of data security legislation. But levels of security are determined in a national market and firms such as ChoicePoint and CardSystems are not going to maintain different levels of security for residents of California than for residents of New York. In a truly federal system citizens with greater preferences for security would pay for this security. But in this market, where firms maintain the same level of security for all individuals, individuals in states with a greater preference for security can impose the costs of these preferences on the entire country.

Federalism would seem to be possible only for regulations that apply to the information practices of businesses small enough to operate within one state. But the publicized security breaches have been for firms that operate nationally and internationally. Adopting a federalist approach to the regulation of these firms does not seem feasible.

B. Benefits of Preemption

1. Inconsistencies in State Statutes

The laws already in place at the state level have major inconsistencies with respect to critical provisions: the definition of personal data; when notice is required; and who must be notified:[14]

Definition of personal data. In California "personal data" include computerized data containing name; social security number; drivers' license number; and account number with access code. Other state statutes include these data in their definitions, but add additional items. In Texas, personal data include unique biometric data. In Arkansas, personal data include some medical data. In Ohio, all personal data, not merely computerized data, are covered by the law. In Montana, all data are covered and data include passport number and insurance policy number. In Georgia, only data held by information brokers are covered (perhaps in response to ChoicePoint which is an information broker and a Georgia firm). Breaches involving encrypted data are exempt from notification requirements in California, but other states differ. In New York notice is required if data are encrypted but an encryption key is also acquired by the thieves. If we assume that the most restrictive laws will govern, then notice will be required for all data (computerized or not) including biometric data and passport and insurance policy number and including encrypted data if the key is also stolen. In other words, the actual policy will be a mixture of the most restrictive aspects of each state policy, so that it will be more restrictive than any one state.

[14] Information on a sate by state basis is available at http://www.ncsl.org/programs/lis/CIP/priv/breach.htm. This site has links to bills and was used in examining the laws discussed in this section. We do not provide a comprehensive analysis of the various statutes; the only point we are making is that even a casual reading indicates that the laws differ in economically significant ways which will greatly increase costs of compliance.

When notification is required. Most states allow for a delay in notice for the purposes of cooperating with a law enforcement agency. However, the Illinois law does not allow such a delay.[15] Most states allow delay while the firm determines the scope of the breach and makes an effort to restore the security of the data; California does not.[16] This means that in California notice must occur while firms are still determining what has been stolen and while security flaws have not been fixed, which could trigger more invasions. Connecticut allows an exemption if the business, after consultation with federal, state and local agencies, determines the breach will not likely result in harm, and in Washington a firm need not disclose a technical breach that does not seem reasonably likely to subject customers to risk of criminal activity. While these two exemptions are reasonable, the fact that only two states have them means that they will not provide any benefits in practice.

Type of notification required. In California, consumers must be notified about a breach. In New York, notice must include a description of the categories of data involved. In many states, in addition to notifying consumers, the credit bureaus must also be notified, but the rules triggering this notice vary. In Indiana and Nevada credit bureaus must be notified if more than 1,000 records are compromised; in New York, 5,000 records; and in Texas and Georgia, 10,000 records are needed to trigger this notice. The result will be that consumers in all states will be notified and will be given a description of all data, and credit bureaus will also be notified if more than 1000 individuals are involved.

Moreover, this set of requirements is based on thirteen states. As additional states pass laws, requirements will shift, and as states modify their laws, they will shift again. Thus, firms will be forced to monitor fifty state legislatures to determine what set of requirements is most restrictive at any time.

2. *The Effect of the Inconsistencies*

We argued above that a federalist approach is not really feasible in this market—that for companies operating at the national level the most stringent set of rules will be binding. Thus, for the most part, we do not envision a situation in which companies will be faced with the prospect of complying with 50 different sets of rules. Nevertheless, companies potentially will be faced with the prospect of familiarizing themselves with all those rules, to make sure they are in compliance. The costs associated with this, which probably do not vary much with firm size, would constitute a particular burden for smaller firms.

Notwithstanding the tendency to gravitate to the most stringent set of requirements, there are some inconsistencies that could be costly. For example, all state statutes have a provision that "alternative notice" (emails, posting on a website, notification of major media) is allowed if individual notice is above certain trigger

[15] This may be an oversight, but it is not mentioned in the Illinois statute.
[16] This may be something learned after the California law was adopted, and may be a benefit of Federalism.

levels—generally 500,000 consumers or a cost of $250,000. But there seems to be no coordination of this requirement across states. Thus, if 450,000 consumers in each state are involved and the cost in each state of individual notice is $200,000 a firm might end up being forced to notify 22.5 million consumers at a cost of $10 million.

These multiple state rules, even if the same, may also lead to confusion among victims. Take, for example, the case where two states both allow alternate notice if more than 500,000 consumers are involved, as the California law does. In State A, 200,000 consumers are involved, so written notices are sent out; in State B, 600,000 consumers are involved, so a notice is posted on the website of the business, an acceptable form of "alternate" notice. Faced with these notices, a consumer in State A could easily assume that two separate breaches have occurred since he will receive a written notice and also see the website warning.

In one draft federal bill,[17] alternate notice is allowed if more than 500,000 consumers are involved or if the cost of direct notices is more than $500,000. This provision itself could save firms (and thus consumers) millions of dollars and lead to reduced confusion.

C. The Benefits of Federalism vs. the Benefits of Preemption

As we discussed above, a true federalist approach does not really seem to be feasible in this market, which is national in scope. The proliferation in state laws will yield some inconsistencies that will impose costs on firms and consumers. But as much as possible, firms will react by complying with the most stringent set of regulations. It is better to have this policy set at the national level, by lawmakers who presumably are representative of the nation as a whole, rather than have one state or one set of states "preempt" policies for the rest of the country.

IX. CONCLUSION

A series of highly publicized data security breaches have created the perception that identity theft and related frauds are a large and growing problem, in need of a new regulatory solution. But, this perception is not borne out by the actual data, which indicate that, depending on the time period and measure used, identity theft has been either constant or diminishing over time. Thus, calls for new regulation should be treated with some skepticism.

It should not be surprising that the market seems to be working fairly well to restrain identity theft. Firms in the credit industry bear most of its costs and have a strong incentive to keep those costs under control.

The major finding of this study is that the costs of a notification requirement are likely to be substantially higher than the benefits. Even for consumers whose data has been compromised, the probability of being a victim of fraud is so low—only 2 percent—

[17] Notification of Risk to Personal Data Act, S. 751.

that little action is justified. Overall, we estimate that the expected benefits of mandatory notification are very small—less than $10 per compromised individual.

The major regulatory costs to be concerned about are not the direct costs of notification. Rather, they are the costs incurred when consumers and firms overreact and take actions that are harmful to themselves and to the free flow of information. Consumers, for example, may be induced to place fraud alerts on their accounts or close them entirely, actions that are likely to be far more costly than being an identity theft victim. They may also be induced to shift their credit transactions offline, which the data show would actually increase their exposure to identity theft.

Firms in the information business may start limiting access to their information in an effort to protect their reputations. But this information is valuable to consumers and the economy and restricting it can have significant costs.

Because a notification mandate is dubious on benefit-cost grounds, it should be carefully targeted to those individuals most at risk in order to increase its potential benefits. Federal preemption of inconsistent state requirements will lower its costs. While these measures can help the benefit-cost balance, it is doubtful that they will be sufficient to bring that balance to the point where the benefits of notification mandate will be sufficient to offset the costs.

REFERENCES:

Bank, David and Don Clark (2005), Visa sets antifraud system upgrade, Wall Street Journal, June 13, p. B4.

Bryan-Low, Cassell (2005), Identity thieves organize, Wall Street Journal, April 7, p. B1.

Bureau of Labor Statistics (2005), Real earnings in May 2005, press release, June 15.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb and Lei Zhou (2003), The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security, 11, 431-448.

Dash, Eric and Tom Zeller (2005), MasterCard says 40 million files are put at risk," New York Times, June 18.

Federal Trade Commission (n.d.), Take charge: Fighting back against identity theft, available on the FTC website.

Federal Trade Commission (2005), Identity theft survey report, Synovate, September, available on the FTC website.

Fountain, Henry (2005), Worry, but don't stress out," New York Times, June 26, Section 4, p. 1.

Garg, Ashish, Jeffrey Curtis, and Hilary Halper (2003), Quantifying the financial impact of IT security breaches," Information Management & Computer Security, 11/2, 74-83.

Jarrell, G. and Peltzman, S, (1985), The impact of product recalls on the wealth of sellers, Journal of Political Economy, 93, 512-536.

Javelin Strategy & Research (2005), 2005 identity fraud survey report (abbreviated summary available online).

Morriss, Andrew P. and Jason Korosec (2005), Private dispute resolution in the card context: structure, reputation, and incentives," Case Research Paper Series in Legal Studies, Working Paper 05-12, June, available at http://ssrn.com/abstract=735283.

New York Times (2005), Company news: LexisNexis restricts access to personal data," March 19, nytimes.com.

Nilson Report (2005), Credit card fraud in the U.S., March, partially available online.

Pacelle, Mitchell (2005), How MasterCard fights against identity thieves, Wall Street Journal, May 9, p. B1.

Pacelle, Mitchell and Christopher Conkey (2005), Card Industry Fights Breach Bills, Wall Street Journal, June 23, p. C1.

Peltzman, S. (1981), The effects of FTC advertising regulation, Journal of Law and Economics, 24, 403-448.

Pegoro, Rob (2005), Voluntary disclosure is the threat to password security," Washington Post, June 12, p. F 7.

Rubin, Paul H. and Thomas M. Lenard (2002), Privacy and the commercial use of private information, Boston, Kluwer Academic Publishers and the Progress and Freedom Foundation.

Rubin, P.H., R.D. Murphy and G. Jarrell (1988), Risky products, risky stocks, Regulation, 35-39.

Sidel, Robin and Mitchell Pacelle (2005), Credit-Card breach tests banking industry's defenses," Wall Street Journal, June 21, p. C1.

Solove, Daniel J. and Chris Jay Hoofnagle (2005), A model regime of privacy protection: Version 2.0, available from SSRN.com.

Wall Street Journal Online (2005), Without a trace: A Wall Street Journal online news roundup, April 20.

Zeller, Tom (2005), Black market in stolen credit card data thrives on Internet," New York Times, June 21.

The Progress & Freedom Foundation is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and civil liberties. The Foundation disseminates the results of its work through books, studies, seminars, conferences and electronic media of all forms. Established in 1993, it is a private, non-profit, non-partisan organization supported by tax-deductible donations from corporations, foundations and individuals. PFF does not engage in lobbying activities or take positions on legislation. The views expressed here are those of the authors, and do not necessarily represent the views of the Foundation, its Board of Directors, officers or staff.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
voice: 202/289-8928 ■ fax: 202/289-6079 ■ e-mail: mail@pff.org ■ web: www.pff.org

Chairman Akin, Ranking Member Bordallo, 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. Two House bills on data protection require consumer notification of a breach and mandate 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 the 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 Protection Regulation is 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. Just last week, the Securities Exchange Commission 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.

In 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. Last July, 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. Last year, 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 nearly 30 states 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 several months, I've worked with businesses of all sizes to educate state lawmakers regarding security breach notification legislation. While not calling for new laws, most in industry acknowledge there are potential benefits to requiring notice of data security breaches:

- The requirement to notify could be 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. Moreover, businesses face the costs of lawsuits for actual damages occurring as a result of data security breaches.
- 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 the victim actually knows, so notification isn't 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 trigger for notice obligations, seeking a "safe harbor" for safe data practices such as encrypting or redacting sensitive data, or storing account data 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 notice 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 30 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."*[6] Any business—large or small—that handles data from customers in many states needs a national standard to mitigate the patchwork of nearly 30 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.

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 identify theft wolves, but business will have every incentive to overbuild to reduce regulatory risk.

---

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

There are two leading House bills related to notification and data protection: The Financial Data Protection Act of 2006 (HR 3997); and the Data Accountability and Trust Act (HR 4127). The small business perspective on these bills is presented next.

Many small businesses would be regulated for the first time

Both bills significantly expand which businesses are covered by data protection requirements. HR 3997 would potentially treat many previously unregulated small businesses as FINANCIAL INSTITUTIONS, with a definition that includes, "*any person that is maintaining, receiving, or communicating sensitive financial personal information on an ongoing basis for the purposes of engaging in interstate commerce.*" HR 4127 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 definitions could cover any sales or service business that records its customers' payment methods or stores any quantity of historical payment transactions.

State notification laws would be preempted by a national standard

HR 3997 creates a uniform national data protection standard by broadly preempting state data security law. It overrides state law that regulates the security or confidentiality of consumer information, safeguarding requirements, and investigation or mitigation mandates for data breaches. HR 4127 supersedes state regulation of information safeguards and notice for unauthorized data access. Both these bills contain preemption language that is stricter than that in GLB, which allowed states to add more stringent rules if they do not conflict with federal rules. Both these bills would therefore provide a welcome national standard to replace a patchwork of state laws.

Penalties could be fatal for small businesses

HR 3997 relies exclusively upon federal agencies for enforcement. These agencies include the FTC, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS).[7] Penalties for violations under HR 3997 are calculated by the particular agency enforcing the act.

[7] Other agencies with enforcement powers under HR 3997 include the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), the Office of Federal Housing Enterprise Oversight (OFHEO) and the Federal Housing Finance Board (FHFB).

HR 4127 authorizes the FTC to enforce requirements for security breach notifications and data safeguards, in accordance with the FTC Act. HR 4127 also extends civil enforcement powers to State Attorneys General to bring suit on behalf of consumers in U.S. District Court. However, this state AG authority is eliminated against defendants already named in a pending civil action brought by a federal agency.

HR 4127 creates a separate penalty scheme for violations of safeguard and notification rules. For safeguard rule violations, civil penalties under HR 4127 are calculated by multiplying the number of violations by an amount not greater than $11,000. Each day of noncompliance is treated as a separate violation. Penalties for violations of the notification rules are calculated in the same manner as safeguard violations, 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 not 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) makes 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 may require notification of law enforcement when network intrusions are recorded by security software monitors, without knowing whether personal information was acquired.

GLB-style Safeguards Won't Work for Small Business

Pending legislation in the House would deliver much-needed relief from state patchwork of breach notification laws. But this preemption comes at a cost, since Congress would add regulation for both notice and data protection safeguards. This tradeoff is only worthwhile if data safeguards are workable for small business.

Realistically, data protection legislation may not be justified, based on a balance between its effectiveness and regulatory burdens. Businesses already have powerful incentives to protect their customers' data. A national notice mandate by itself may be enough to enable market forces to discipline businesses that fail to protect customer data.

Security mandates will undoubtedly bring 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 few 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

---

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

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:

- A small business owner isn't even going to be aware of new safeguard requirements if it's in a previously unregulated industry. Many owners will learn for the first time that they are subject to new regulations through advertising and marketing by 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).
- 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 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

---

[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

[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

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.

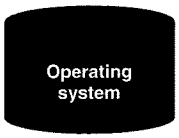
Moreover, until regulators have published approved best practices suitable and affordable for small business compliance, please consider a temporary exemption from new data protection requirements for small entities—especially those businesses who were previously not covered by a federal functional regulator.

APPENDIX A: The Security Stack

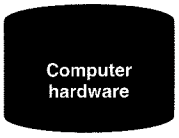
Responses to security threats happen at multiple layers of a "security stack" that starts with user behavior, includes hardware and software solutions, and rests on a foundation of network security.

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.

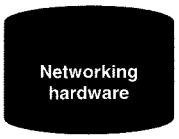
Application software includes productivity tools such as e-mail, word processors, spreadsheets, databases, instant messaging, browsers, firewalls, and anti-virus software. In the late 1990's, the application layer was often attacked with viruses propagating through vulnerabilities in e-mail clients or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

Prepared Testimony of

Harry Dinham, President Elect

National Association of Mortgage Brokers

on

Data Protection and the Consumer; Who Loses When Your Data Takes a Hike?

before the

House Committee on Small Business
Subcommittee on Regulatory Reform and Oversight

Committee on Small Business

Tuesday May 23, 2006

Good morning Chairman Akin and members of the subcommittee, I am Harry Dinham, President Elect of the National Association of Mortgage Brokers ("NAMB"). Thank you for inviting NAMB to testify today on the potential burdens placed on small businesses by proposed data security legislation.

NAMB is the only national trade association exclusively devoted to representing the mortgage brokerage industry. As the voice of the mortgage brokers, NAMB speaks on behalf of more than 25,000 members in all 50 states and the District of Columbia.

America enjoys an all-time record rate of homeownership today. Mortgage brokers have contributed to this achievement as we work with a large array of homebuyers and capital sources to originate the majority of residential loans in the United States. At the end of last year, the overall homeownership rate neared 70%. Many families still need assistance in obtaining homeownership and NAMB members will be there to help them. However, with increased regulatory burdens and costly requirements being placed on small businesses, such as certain proposed data security provisions currently

contemplated by Congress, we are concerned that many mortgage brokers could be forced out of business.

NAMB is fully aware that identity theft remains one of the fastest growing crimes in America. Working with consumers directly on a daily basis, we appreciate the dire consequences of identity theft. Identity theft is a crime that does not discriminate, can occur at any time, and despite meticulous efforts to protect one's personal information, is not fully preventable. Identity theft victims suffer not only emotionally, but also financially, often unable to qualify for a mortgage because they are left with blemished credit histories as a result of the thieves' actions. Clearly, efforts to protect against identity theft are necessary, and we commend Congress for taking action on the many issues surrounding identity theft and data security. Equally important to actions taken to halt the growing incidence of identity theft, however, is the awareness that proposed measures should not have the unintended consequence of harming the small businesses of America that are so vital to our communities and economy as a whole.

For this reason, NAMB supports federal legislation that establishes a uniform, national standard for investigation and notification of data security breaches, but which is cognizant of the time and cost limitations that small businesses face. NAMB believes that any proposed data security breach legislation must complement, but not otherwise duplicate or override, existing legislative and regulatory schemes that safeguard sensitive consumer information against identity theft. NAMB looks forward to working with Congress to ensure that any such proposed legislation creates targeted and meaningful consumer protection measures that aid in identifying and protecting against identity theft, but do not disrupt or otherwise impede the economic health of small businesses serving the financial services marketplace.

NAMB has three principal areas of concern regarding proposed data security legislation: (1) the lack of uniformity and clarity caused by the current state patchwork of laws; (2) credit freeze provisions, which place small businesses at a competitive disadvantage and fail to afford consumers meaningful protection; and (3) the time and cost burdens placed on small businesses by the "file monitoring" provision.

I. STATE PATCHWORK OF LAWS

The current patchwork of state laws on data security protection and breach notification laws is confusing, cumbersome, and unduly costly for small business providers of financial services.

California led the way in 2003 with the first security breach notification law entitled "Notice of Security Breach" (SB 1386). Under SB 1386,[1] both businesses and government entities must notify customers "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." A security breach is defined broadly as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information

[1] *See* CA Civil Code Section 1798.29 and 1798.82.

maintained by the person or business." Significantly, SB 1386 does not define the term "unauthorized," and for this reason, the trigger for notification is considered to be both vague and broad. The lack of clarity in California's notification provision makes compliance difficult and causes uncertainty for many small businesses struggling to understand and implement the law to the benefit of their consumers.

SB 1386 became effective in 2004. Since that time, according to the National Conference of State Legislatures, numerous state have introduced legislation on security breach notification. As of today, at least 30 states have enacted security breach notification laws, many of them using the California law as a model: Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Washington and Wisconsin.

These multiple state laws create a regulatory framework that is unduly burdensome and complicated for small businesses that have limited resources and time. NAMB believes that a uniform, national standard for data breach investigation and notification will enable small businesses to protect their consumers' sensitive personal information manner effectively and in a cost-efficient manner.

II. CREDIT FREEZE PROVISIONS

Adding to the issues raised by the various state security breach notification laws is the recent state trend of enabling consumers to lock their credit files—often referred to as "credit freeze" or "security freeze" laws. There are a number of initiatives to address the issue of identity theft and fraud that small businesses must already understand and incorporate into their daily business routines, such as the fraud alert. But "credit freeze" laws prove to be especially burdensome to small businesses and yet fail to offer consumers meaningful protection against identity theft.

Today, at least 12 states have a "credit freeze" or "security freeze" law on their books. Many more states are contemplating passing similar legislation.[2] Credit freeze laws allow identity theft victims, and in some states *any consumer*, to place a "freeze" on their credit reports. As a result, these laws can alter the state credit reporting systems significantly and have a detrimental impact on a consumer's ability to secure credit quickly and effectively.

The Mechanics of a Credit Freeze Law

With credit freeze legislation, a consumer can request in writing that a consumer reporting agency "CRA" place a freeze on his or her credit file. The CRAs generally have

[2] As of this printing, the following 12 states have credit freeze laws: California, Colorado, Connecticut, Illinois, Louisiana, Maine, Nevada, New Jersey, North Carolina, Texas, Vermont and Washington.

five business days to comply with the consumer's request. Within five business days of putting the credit freeze in place, the consumer must then receive written confirmation that the CRA has complied with his or her request. The written confirmation provides the consumer with a password or other unique identifier that must be used each time the consumer wants to release any credit information from his or her file. Once a credit freeze is placed on the credit file, the CRA may not release any credit information on that consumer to a third party, except with the consumer's express, written authorization.

However, certain exceptions to the credit freeze exist. For example, CRAs still can comply with requests for credit information if related to law enforcement or child support reasons. There also is a clear exception provided for *existing business relationships*. The consumer does have the ability to remove the security freeze at a later date. Any request by a consumer to "thaw" the credit freeze placed on the credit file must be sent in writing to each CRA with the correct PIN. In addition, certain states may charge a fee each time a consumer imposes or lifts the freeze. Consumers who are identity theft victims, however, do not have to pay these fees. In essence, any consumer that has a credit freeze on his or her credit file will be unable to open a new credit card account, apply for insurance, make an application for a new bank account, or take out a mortgage loan instantaneously. A freeze on a credit file eliminates any "point-of-sale" transactions because it can take as many as three days to remove the freeze once the consumer has notified the CRA to "thaw" the file.

Consequences of the Credit Freeze

The net impact of consumers placing freezes on their credit files can be disastrous for anyone conducting business in the credit industry – small business mortgage brokers not excluded. Consumers use and access credit information everyday and the need to secure that information quickly can be vital to consumers achieving his or her dream of homeownership. Many mortgage loan transactions occur in a matter of hours, not days. Imagine a customer that wants to put a bid on a house where intense competition is expected. If he or she has a credit freeze in place, it can take *days* to remove that freeze in order for small business finance market participants to access the needed information to approve a loan—days that a consumer does not have in a fast-moving housing market.

The efficacy of these laws as a protective tool against identity theft is also up for debate. For example, many of these laws fail to remove the consumer's name from appearing on prescreened target lists sold by the national CRAs to various furnishers of credit or insurance,[3] leaving consumers vulnerable to fraud despite placement of a freeze.

Moreover, an unintended consequence with these state credit freeze laws is that small businesses are placed at a competitive disadvantage compared to financial institutions

[3] Further exacerbating this problem is the fact that these prescreened lists are often being sold to third-party entities who may not have a clear "permissible purpose", as defined in FCRA, to access the information. Of course, this issue can be dealt with directly by simply enforcing FCRA and ensuring that an entity having access to a pre-screened list actually has a permissible purpose.

where the consumers have preexisting accounts because pre-existing business relationships are exempt from the credit freeze. For example, the mortgage division of a bank that the consumer already has a relationship with can still access such consumer's credit file. This pre-existing business relationship gives the bank's mortgage division a decisive, competitive advantage over a mortgage broker.

Most importantly, consumers already have a myriad of other laws that offer similar, and perhaps even greater, protection against identity theft and fraud. One of the most comprehensive national privacy laws in existence today is the Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act of 2003 "FCRA". FCRA governs the nation's credit reporting system and puts in place specific restrictions on who can access a consumer's credit file and under what circumstances. FCRA also enables consumers to obtain their credit reports at any time, and affords them the opportunity to dispute any information they feel may be inaccurate.

For example, today an identity theft victim can contact a CRA, provide a copy of the filed police report and request that an extended fraud alert be placed in his or her credit file. That request will automatically remove the consumer's name (*i.e.*, opt out) from pre-screened credit card and insurance offer lists and give the consumer two free credit reports over the next 12 months to check for any fraudulent activity. The opt out request also mandates that the CRA block any further reporting of credit information on accounts created or negatively impacted due to fraud or identity theft. This fraud alert serves as clear notification to any potential creditor that the consumer has previously been a victim of identity theft and that certain additional precautions are necessary before granting credit. Under FCRA, both CRAs and creditors must comply with the laws that afford consumers these protective measures and impose liability for any breach of compliance. For example, a creditor can be sued by the Federal Trade Commission, the states attorney general or the consumer for noncompliance with FCRA.

The protective measures already in place, such as the fraud alert, must be given a chance to be effective in safeguarding consumers' credit information. Proposed legislation should not include a credit freeze provision because it inhibits small business mortgage brokers from accessing a borrower's credit report in time-sensitive transactions, which in turn reduces competition in the marketplace, restricts consumer choice, and increases costs to consumers.

III. FILE MONITORING PROVISIONS

File monitoring provisions allow consumers to receive file monitoring services from credit bureaus when confidential consumer data has been breached. Proposed legislation should not require small businesses to file monitoring to consumers because it creates undue administrative burdens and significant costs for small businesses, such as mortgage brokers, and fails to provide a meaningful benefit to consumers.

File monitoring provisions do not *prevent* identity theft, but only mitigate the effect of such fraud afterwards. The provision is not useful, effective or necessary for the

following reasons: (1) CRAs often do not report recent credit activity for up to 60 days; (2) consumers receive a free credit report from each CRA annually and therefore, can obtain a free credit report almost every quarter from each of the CRAs; (3) a consumer reporter is already required to inform the consumer through a clear and conspicuous notice of their right to obtain free credit reports from each CRA and provide information necessary to exercise such right; and (4) file monitoring operates on the presumption that mandatory reporting occurs, but this requirement will only capture those entities that are compliant with reporting requirements and not the bad actors who fail to report in the first instance.

The overall benefit to consumers *versus* the significant cost and administrative burden placed on small businesses, such as mortgage brokers, is unclear. The SBA recently released a study on compliance costs that found small businesses, including mortgage brokers with fewer than 20 employees, spend about $2,400, or 45%, more per employee to comply with federal regulations than their larger counterparts (firms with 500 or more employees). For this reason, NAMB supports provisions in any proposed legislation that would increase the Small Business Administration's regulatory oversight when implementing regulations are issued.

NAMB supports legislative proposals that would enable the functional regulatory agency to exempt small businesses in a fair manner while at the same time protecting consumer interests. To aid the agency, Congress should incorporate factors or guidelines in the legislation that must be considered by the functional regulatory agency. For example, the legislation can provide that an exemption from file monitoring is required for small business mortgage brokers that are under a certain size or have a limited volume of loans (*i.e.* revenue) per year.

At a minimum, NAMB recommends that file monitoring services be provided *only if* a consumer has already exercised their right to obtain their free credit report from each of the CRAs for that calendar year. Congress should also provide regulatory authority to place price caps that can be charged to the small business mortgage broker for such monitoring service. Congress should also provide the regulator with authority to create provisions that allow small businesses to have in place measures to prevent identity theft, above and beyond the Safeguards Rule requirements under the Gramm-Leach-Bliley Act, which would alleviate the need for file monitoring. The legislation should create a 'safe harbor' for any liability that could potentially arise from maintaining all the records necessary to conduct file monitoring. In short, any proposed file monitoring provision should be crafted so that it does not prove costly and unduly burdensome for small businesses. To do otherwise will only increase consumer costs significantly.

CONCLUSION

NAMB appreciates the opportunity to offer our views on the impact on small business from current legislative proposals dealing with date security. I am happy to answer any questions.

○