AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CREDIT CARD DATA PROCESSING: HOW SECURE IS IT?

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JULY 21, 2005

Printed for the use of the Committee on Financial Services

Serial No. 109–48

U.S. GOVERNMENT PRINTING OFFICE

29–461 PDF WASHINGTON : 2006

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

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

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

BERNARD SANDERS, Vermont

Robert U. Foster, III, *Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

SUE W. KELLY, New York, *Chair*

RON PAUL, Texas, *Vice Chairman*
EDWARD R. ROYCE, California
STEVEN C. LATOURETTE, Ohio
MARK R. KENNEDY, Minnesota
SCOTT GARRETT, New Jersey
J. GRESHAM BARRETT, South Carolina
TOM PRICE, Georgia
MICHAEL G. FITZPATRICK, Pennsylvania
GEOFF DAVIS, Kentucky
PATRICK T. MCHENRY, North Carolina
MICHAEL G. OXLEY, Ohio

LUIS V. GUTIERREZ, Illinois
DENNIS MOORE, Kansas
CAROLYN B. MALONEY, New York
STEPHEN F. LYNCH, Massachusetts
ARTUR DAVIS, Alabama
EMANUEL CLEAVER, Missouri
DAVID SCOTT, Georgia
DEBBIE WASSERMAN SCHULTZ, Florida
GWEN MOORE, Wisconsin
BARNEY FRANK, Massachusetts

CONTENTS

CREDIT CARD DATA PROCESSING: HOW SECURE IS IT?

Thursday, July 21, 2005

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:13 a.m., in room 2128, Rayburn House Office Building, Hon. Sue Kelly [chairwoman of the subcommittee] presiding.

Present: Representatives Kelly, Pryce, Bachus, Castle, Kennedy, Garrett, Renzi, Price, McHenry, Gutierrez, Maloney, Hooley, Moore of Kansas, Matheson, Scott, Davis of Alabama, and Cleaver.

Chairwoman KELLY. I call this hearing on the Subcommittee on Oversight and Investigations to order.

Over the last few months, disturbing information has come to light about breaches in data security across the financial services industry. Millions of consumers have found out that their personal information may have been compromised. Millions more are now worried about personal data protection with the attention given these breaches.

This is an issue that personally affects all of us. In cities and towns across my congressional district in New York and all across our country, we rely on credit cards day in and day out. We expect nothing less than a safe and secure system of processing them.

These breaches harm the network of financial transactions that gives the United States the most productive economy in the world. These breaches cause consumers to lose confidence in the payment systems that drive sales growth. They impose new risks and costs on merchants and threaten some with the loss of customers and their livelihood. We need to do everything possible to ensure that our personal information remains privileged and protected when we make any financial transaction.

Today's hearing will deal specifically with the recent data breach at CardSystems where more than 40 million credit card accounts of 4 major credit card brands may have been exposed. At least 200,000 accounts were definitely stolen, and evidence exists that a routine may have been in place to allow the culling of credit card information on a regular basis.

In response to these breaches, Visa and American Express are terminating their relationship with CardSystems, while the company itself is putting in new measures to ensure data security.

Yesterday, in testimony to the Financial Services Committee, Federal Reserve Chairman Greenspan noted that increased regula-

tions may have the consequence of killing the electronic innovation and productivity that have kept our economy and our markets growing. He also noted that in a free market economy all companies that hold personal data have a huge financial incentive to keep it as secure as possible. Unfortunately, in this case and others, those incentives either failed or were overcome by the financial incentives of fees.

What we need to learn today from the witnesses in this case is, what happened, what was supposed to happen, and what can be done to prevent this from happening again.

I welcome the witnesses, and I yield now to the gentleman from Illinois.

Mr. GUTIERREZ. Good morning. I want to thank Chairwoman Kelly for calling this hearing entitled, "Credit Card Data Processing: How Secure Is It?" I think the answer to many people reading the news lately is, not secure enough.

Data security is very important to many of us here on this committee, and I am pleased that we will be joined later on by some of our colleagues who will ask to participate.

This issue is also personally important to me. I am proud to have served as a conferee on the FACT Act, which dealt with similar issues.

In March, I coauthored a bill with Congresswoman Melissa Bean on this issue, and I am proud to be an original cosponsor of the recent bill introduced by Representatives Bean and Artur Davis. There are many other worthy bills on this topic, and I suspect we are going to be working together to craft a solution before the end of the year.

We need to understand what happened here and where the gaps in the law are so they can be fixed. We also need to determine the proper way to notify and protect consumers and inform the credit rating agencies when consumer data compromise can lead to identity theft. We need to make sure that consumer notification takes place in language the consumer can understand.

I look forward to hearing from the witnesses so that we can learn from the problems they experience and minimize similar occurrences. At the proper time, I will inquire about the audit processes or credit processes and how CardSystems could have been certified while maintaining an adequate software and retaining customer data in violation of its Visa contract.

Additional checks and balances may be necessary in the system of certification. The largest banks, I am told, have supervision in the form of professional examiners from their regulator onsite every day of the year. It might make sense to employ a similar process when we are talking about security of large amounts of data in an entity that is not a bank but is performing functions of a bank. It would also be helpful to determine the actual scope of the compromised data and the degree of fraudulent activity that may be related to this incident.

I am pleased to welcome all of the witnesses, and I especially want to welcome Evan Hendricks whose quarter century of expertise proved invaluable during consideration of the FACT Act issues, and I am certain he will be helpful today. I understand that he has

a plane to catch early this afternoon, but we are especially grateful that he could make the time to be with us today.

Thank you so much, Mr. Hendricks, for being here.

We have been joined by Mr. Matheson, and I ask unanimous consent that he be permitted to make an opening statement.

Chairwoman KELLY. So moved.

We have been joined by a number of members who are not on this particular subcommittee but that are on the Financial Services Committee as a whole. We are honored by their presence. We have Mr. Kennedy, Mr. Castle, and Mr. Bachus with us this morning, and I ask unanimous consent that they too may be able to make an opening statement. So moved.

So without objection, all members' opening statements will be made part of the record.

I turn now to Mr. Garrett.

Mr. GARRETT. Thank you, Madam Chairwoman, for holding today's hearing on data security and credit card systems in light of recent headlines. I think it is both timely and necessary that we have these hearings, not only so that we can learn more about the apparent data breach at CardSystems affecting the four major credit card companies, but also we can learn how this committee may be able to respond in an appropriate manner.

The data breaches that were recently disclosed by financial institutions have generally, in the past, involved lost data tapes or similar mishaps which do not necessarily suggest criminal intent. However, in this circumstance it appears that someone was able to compromise their database system to obtain information for malicious purposes.

So while the other types of data breaches are obviously cause for concern, it is especially troubling when we learn that sensitive information has fallen into the hands of apparent criminals. Therefore, I am particularly interested in learning about how consumers are protected against credit card fraud or other problems resulting from this breach.

I think we also need to examine how the breach at CardSystems could have been avoided. Is there a shortfall in the law? Do we need new laws? Or do companies simply need to be more responsible in complying with existing laws and any of their contractual obligations?

My hunch is that CardSystems' apparent lack of an adequate data security regime may simply be that they were running crosswise with existing laws or contractual obligations. So we simply need to learn now how the existing lay of the land has been applied in this situation before we move on and consider making more laws.

I think we also may want to use this as an opportunity to at least explore and understand a little bit what potential impact the decisions that may affect CardSystems' future may also have indirectly on any of their vendors or other players in the system.

I would also like to say for the record that I appreciate MasterCard's efforts to bring the situation at CardSystems to light, as they were under really no direct obligation to do so, but I think that they did so in thinking what was most responsible for getting the information out in the interest of their cardholders. And for

that reason, I believe that they should be commended for their actions.

Thank you again, Madam Chairwoman, for holding this hearing, and I yield back the balance of my time.

Chairwoman KELLY. Thank you.

Ms. Maloney?

Mrs. MALONEY. Thank you very much, Madam Chairwoman, for having this hearing today that continues to address the really very pressing issue of data security and identity theft through this series of hearings.

This hearing focuses on a particularly terrible example of a breach of data security: The exposure of 40 million credit and debit card accounts at a data processing company handling Visa, MasterCard and American Express. Based on an FBI investigation it appears that the data processor, CardSystems, blatantly violated the contractual data security restrictions imposed by each of the credit card companies.

But this would not have come to light had it not been for a huge breach and resultant fraudulent transactions. I expect that each of the credit card companies here today will explain to us that they spend a great deal of time, money and resources preventing credit card fraud and protecting consumers from the effects of credit card fraud through zero liability policies and card reissuance.

This is all very laudable but the issue before the committee today is not just credit card fraud: the issue before us is the much more complex issue of identity theft, because it does not simply involve a fraudulent charge on a card, it is typically the opening of a new account in the name of the victim. Identity theft is harder to find, harder to assess, and harder to combat, but it is the main issue we need to address.

For example, we may have a good idea now of all the credit card fraud that is likely to result from the CardSystems breach, but that does not mean that we know the extent of the identity theft risk.

Similarly, the credit card companies often identify credit card fraud right away, but in this case they appear to have been absolutely clueless for months while personal data was removed from the database.

At present, the main protections against identity theft are contractual agreements between credit card companies and the banks and data processors that handle the information. The CardSystems incident is a spectacular failure of this private sector protection and suggests that more regulation, more enforcement and more penalties are necessary in this area.

For example, until yesterday, it appeared that the credit card companies would continue to do business with CardSystems even though CardSystems had not complied with the data security requirements.

Moreover, there is a huge regulatory gap under Gramm-Leach-Bliley. The respective financial regulators are responsible for making sure that financial institutions who contract out data processing functions ensure their contractor's compliance. And the FTC rules require data processors to preserve the confidentiality of personal financial data. But in this case, the regulators appear to have played "toss the hot potato" with this whole incident.

So far, all the consequences of data security breaches could be viewed by a data processor as the cost of doing business.

Yesterday, perhaps bowing to the pressure of this important hearing, Visa and American Express terminated their business with CardSystems, but MasterCard still has its data processing handled by them. This situation is not acceptable, and we need to provide the legal structure to fix it.

I am a proud cosponsor and original sponsor of this legislation that has been introduced by my colleague, Representative Bean from Illinois, and it is a good first step in this area. I look forward, as always, to hearing the witnesses' views and some of the alternatives and ideas that they may have, and I hope that we can benefit as we move forward with this bill, and I thank all of you for being here. It is extremely important.

I must say that one of the biggest credit card theft rings is in the district that I represent in New York, in Queens, and it is just a terrible problem once it happens, and so our efforts to prevent it are very important. Thank you.

Chairwoman KELLY. Thank you, Ms. Maloney.

Mr. Kennedy?

Mr. Price?

Mr. PRICE. Thank you, Madam Chairwoman. I appreciate the opportunity to participate in this hearing, and I want to thank all of the witnesses for being here.

I want to especially welcome Mr. John Perry of CardSystems, who has a portion of his business in my district. I am sorry I am late but I want to echo the comments of others who have talked about the importance of having security within the credit card system. I am somewhat astounded by some of the comments that I just heard, however, in view of the fact that CardSystems, itself, discovered the breach, notified the companies of the breach, and is working aggressively and actively to correct the challenges that they and the industry have.

Greater regulation and greater penalties I am not certain—which is oftentimes the knee-jerk reaction to a challenge that we have in any area—I am not certain that is indeed the answer at all.

So I look forward to the testimony before us today. I look forward to increasing my knowledge of this area, and I also hope that individuals will lower the rhetoric, calm down, and work toward solutions in this area as opposed to bomb-throwing. And I yield back.

Chairwoman KELLY. Mr. Moore?

Mr. MOORE OF KANSAS. Thank you, Madam Chairwoman. I would like to thank you for holding today's hearing and thank the witnesses for appearing today to share their information with us.

The focus of this morning's hearing is data security within the credit card payment system, specifically the recently publicized data breach at CardSystems Solutions that could have affected approximately 40 million credit and debit card accounts.

I look forward to Mr. Perry's testimony this morning. I appreciate your being here, sir, to discuss what steps CardSystems is taking to secure deficiencies in the system.

The CardSystems breach, among many others of businesses as diverse as data brokers, retailers, and banks, begs the question of what Congress should be doing to protect consumers from identity

theft. As we have all seen over the last few months, States across our country have been enacting or considering data security notification laws to deal with the problem of data breaches.

The proliferation of State activity in the area of data security and notification, though, is now creating a confusing patchwork of conflicting laws that is adding to the cost of doing business nationwide. I think it is time for Congress to act to protect consumers from data breaches and create a uniform national standard that seeks to create a level of certainty for consumers and national businesses.

Representatives Deborah Pryce, Mike Castle, and I have been working on data security legislation that would, for the first time under Federal law, require companies to notify consumers when their sensitive personal information has been accessed in a way that could lead to identity theft. There should be a few guiding principles behind any data security bill that Congress considers.

Number one, companies should be required to safeguard their data. Number two, breached businesses should be required to notify consumers, law enforcement, regulators, and relevant third parties when sensitive personal information is compromised. Number three, breached entities need to ensure that consumers are protected after their data is compromised through credit file monitoring and other such actions. And, number four, Federal preemption, we believe, is necessary to create a meaningful uniform national standard.

Our legislation embodies each of these guiding principles, and we will be introducing our bill today. Additionally, I know you will not believe this but sometimes when Congress sees a problem they overreact, and I hope that—what are you laughing about?

[Laughter.]

I hope that is not the case here, because we do need to address and correct this problem but at the same time not overreact. We have one of the best credit systems in the whole world right here in this country, and it is a benefit to consumers that they can get a quick answer to a credit check. What we do not need, though, is to go too far and hurt the industry which has set up this wonderful credit system.

As Congress considers data security legislation, we need to again correct this problem without overreacting. As this process moves forward, I look forward to continuing to work with Members on both sides of the aisle to pass the best bill we possibly can. This should not be about Republicans and Democrats, it should not be partisan at all. We need to address this in a bipartisan fashion, and I am confident we can do that here. I am very proud of our committee, because we have worked well together in other areas in the past, and I believe we can do that here.

Thank you again, Chairwoman Kelly. I look forward to hearing from our witnesses.

Chairwoman KELLY. Thank you very much.

Mr. McHenry?

Mr. MCHENRY. Thank you, Madam Chairwoman. Thank you so much for having this hearing today, and I appreciate your leadership on this issue.

I will make this brief because I know we have a lot of testimony to hear. The last time I saw this many witnesses lined up at a table before a hearing we had baseball players in. So, Mr. Sosa, Mr. McGwire, thank you all for being here today.

But in all seriousness, data security should be a top concern of all financial institutions and all financial service industry related folks. And what I would like to examine is what is being done now. I would also like to examine whether or not there are market forces that would influence how you protect data.

I do not think that the government should step in when the market can actually dictate, and I think there are repercussions for companies that do not protect data. I think there are repercussions financially on their bottom line for companies that do not do what is appropriate and right and do not secure data appropriately. Customers will leave, merchants will refuse to deal with you, and the market will deal with it.

Now, does the government need to intervene if the marketplace is going to deal with companies on these issues? That is what we need to understand as a committee, and we need to see where we need to go. If there is a marketplace that is going to determine data security, government intervention may hurt in this regard and actually may have an adverse effect on data security rather than the true spirit of what we would attempt to do as a government.

So I welcome the testimony today. I look forward to hearing from all of you and look forward to hearing what has happened and actually what is occurring currently and what you view as the best way to secure data going forward. Thanks so much.

Chairwoman KELLY. Thank you.

Mr. Davis?

Mr. DAVIS OF ALABAMA. Thank you, Madam Chairwoman, for calling this hearing, and I am going to try to follow Mr. McHenry's lead and be somewhat brief, given the fact there are so many of you and a lot of us who are here to question you. Let me just make a few general observations.

The first one, one of the happy things, I suppose, about this kind of climate is that the industry, frankly, has as much of an incentive to have this institution act in a responsible way as the consumer does. I think all of you who are here as industrial representatives and corporate representatives understand that your ability to provide a service to your consumers, your ability to attract consumers is in peril if they do not have confidence in how their information is being handled. That is the bottom line.

So you have the same incentive, and I think that is why Mr. Moore and some of us can confidently say that this should not be a left-right kind of issue, it should not be a business-consumer kind of issue because you are in the same place in terms of wanting to promote consumer confidence.

The second observation that I will make—this is something that I see routinely on this committee—is that the world of financial service transactions now, the world of financial service in general is so numbingly complex that a lot of people that you serve every day and that we serve every day frankly just want to throw up their hands and say, "We do not understand this."

And they feel so detached from their own ability to go out and make purchases and all of a sudden you have this information about security breaches and I am willing to bet that probably makes them feel even more detached. And then, worst-case scenario, they will learn weeks later that there may have been a breach that they did not even know about.

I think we have to speak to that consumer anxiety. I think we have to speak to people who feel that somewhere out there things may be happening that are adverse to their interests that could involve a fraud or a theft and they did not even know for several weeks. We have to speak to that anxiety.

The final point that I will make, Ms. Bean, Mr. Frank, and I are the lead sponsors on a bill that I think all of you are aware of. It is referred to by some in the press as the Democratic bill. I hope that this is the beginning of a conversation that can draw the best instincts from my side of the aisle and the best instincts of our partners on the other side of the aisle

And this committee has done it before. We did it very recently in the context of GSE's, an enormously complex issue. Most people did not think, given the acrimony of last year's hearings, that we would get to a middle ground on GSE's. We got there. I wish the U.S. Senate would respect the fact that we got there, but we got there.

We got there on the question, because of my colleague from Alabama, Mr. Bachus' leadership, on the extension of the Fair Credit Reporting Act several years ago. Nobody expected us to build a consensus that helps protect the best credit system in the world.

So I drew inspiration from those things.

Again, I thank the chairwoman for having this hearing and look forward to working with all of you.

Chairwoman KELLY. Thank you.

We turn now to Mr. Bachus.

And I would like to say that for the ex officio members, because we have a lot of people here, many opening statements, I am going to ask the people who are ex officio, and we welcome them here, but I am going to ask them to keep their statements to 3 minutes each.

Mr. Bachus?

Mr. BACHUS. I appreciate that, Chairwoman.

As with any legislation that comes before the subcommittee on which I am chairman, it obviously is something of great concern to me, and I commend you for having this hearing and for your leadership over the past several years, not only on this issue but identity theft and credit card fraud.

Credit card fraud, identity theft, and data security breaches are really three different things, and we sometimes have a tendency to mix and match them. But as we go about this hearing, we should bear that in mind.

And I appreciate the remarks of the gentleman from Alabama. The gentleman from Alabama has introduced a bill along with the ranking member, Ms. Bean, and Chairman Pryce and Chairman Castle and Mr. Moore have introduced this morning a bipartisan piece of legislation. And, further, we have had two other members, Mr. LaTourette and Ms. Hooley, who have introduced a third bill.

Mr. Garrett questioned whether existing law is sufficient or do we need new laws? Can we just enforce those laws on the books? A great deal of this is going to be, yes, we just need to enforce what is there.

Law enforcement has a role in this. This was a criminal violation; somebody hacked in. This was a criminal act not by the victim but by a criminal. But I will answer the question, yes, we do need to address this, and I think that the Members' bills, as we go through this, we just need to do, as Mr. Price said, we need to show caution, and I associate myself with his remarks and Mr. Garrett's remarks.

With that, I do want to say two other things, if I could. One, CardSystems Solutions was a victim of a criminal act by a hacker, and they did report this to MasterCard. They voluntarily reported it, and they should be commended for that. That is my understanding.

And, furthermore, I would like to note that we learned of the situation at CardSystems Solution through a public announcement by MasterCard International. This announcement was not required by the law; rather, MasterCard played the role of a good citizen, good corporate citizen in notifying the public of the situation, even though MasterCard itself was not the subject of the breach. And I commend MasterCard for their efforts.

So in the aftermath of this hacking incident, I think the system worked well, and these companies responded in an appropriate way. But I do believe that really the solution to this is that we first in this Congress pass a law, and I know Chairman Castle and Chairman Pryce and others are working on it with Mr. Moore and others and Mr. Davis, on establishing a national uniform standard protecting all Americans.

And with that, I yield back any time I have.

Chairwoman KELLY. Thank you, Mr. Bachus.

Mr. Cleaver has indicated he has no opening statement, so we will turn to Mr. Scott.

Mr. SCOTT. Thank you very much, Chairwoman Kelly, and I want to thank you and Ranking Member Gutierrez for holding this very important hearing on credit card fraud and identity theft.

I certainly also want to take this opportunity to welcome Mr. John Perry, who is president and CEO of CardSystems from Atlanta, Georgia, my hometown.

Of course we all know that recent news continues to affirm the viewpoint by many consumers that their personal credit is constantly at risk for fraud or abuse. It is a major, major problem facing this country. Tens of millions of consumers have been exposed to credit fraud or theft, and these data attacks and frauds have hit major credit card issuers and banks, many of whom already have high standards for data protection.

And in my hometown of Atlanta, some of the major events and incidents have occurred at ChoicePoint and at CardSystems. But it is important to note that ChoicePoint is recovering from its security breaches, and CardSystems has responded to this and they are working their way through the fallout, and I certainly commend you in the steps that you are taking and wish you speedy success.

It is also important to note that the incidence of theft has gained national attention. From my own constituents, for example, we have had many discussions with privacy issues. Many of them are asking what they can do to protect themselves and what Congress can do to punish the credit thieves.

Credit theft and identity fraud can be devastating to a family. Their credit can be ruined, it can take countless hours and resources to repair their good name, and I believe that Congress should provide additional protections that are substantive and not merely reactionary.

I look forward to learning more in this hearing and hearing this distinguished panel. Thank you.

Chairwoman KELLY. Thank you, Mr. Scott.

Chairman Castle?

Mr. CASTLE. Thank you, Chairwoman Kelly. Thank you for allowing me to speak in my 3 minutes, so I will jump right to it, and I will jump out of what I was going to say formally and just talk a little bit about our legislation that has been referenced by several people that Chairwoman Pryce and Dennis Moore and I introduced today.

I believe very strongly that we do need a national solution, and we need it fairly rapidly. There is a lot happening in the States. Maybe there are certain State-relevant things that need to exist, but I think we need to speak to this sooner rather than later. I am delighted we are doing it on a bipartisan basis. Actually, we have bi-legislative basis right now. We have two bills out there, maybe others before we are done, but we are moving forward.

I would like to have compliance. I am not particularly interested in enforcement, but obviously you need the enforcement behind it to get the compliance. But our hope is that once we share information and we have a clear standard, which is something else I want in our legislation, I want everybody to be able to clearly understand what it is that we are doing.

I agree with Chairman Bachus, there is a lot out there now, there are a lot of enforcement mechanisms which are out there now, but we need to make sure that everybody understands what they are dealing with in this particular area.

We need to expand this to entities not under financial regulation now, Gramm-Leach-Bliley and those who regulate under Gramm-Leach-Bliley, because a lot of the breaches that have happened have happened from entities away from that, and that is also significant.

And I think there is an issue of consumer angst here. I was one who received a notice. I did not have much idea of what to do. Eventually, I figured it out. And my concern is who is going to really open that envelope, who is really going to know when you will be mailing it out, the whole business of not over-involving the consumer but making sure the consumer is absolutely protected when the consumer has to be.

Those are at least some of our goals in drafting this. I hope that some day we have this legislation before us and we do it unanimously, quite frankly. I have no interest in having something that is divided in this committee with respect to where we are going.

So we appreciate you being here today. We appreciate your contributions to this information. It is simple to say what I have just said, but it is a little hard to write it, as we have learned. So we know it is complicated, and we are going to need a lot of help to do it, but I think we have a very strong determination, and it is one of those issues that should move forward and it is one of those issues that really should not get hung up on politics but should be able to be resolved fairly rapidly.

And with that, I yield back, Madam Chairwoman.

Chairwoman KELLY. Thank you.

Ms. Wasserman Schultz?

Ms. WASSERMAN SCHULTZ. Thank you, Chairwoman Kelly and Ranking Member Gutierrez, for convening today's important hearing.

I particularly want to welcome Zyg Gorgol from American Express, which is one of the largest employers in my district, in South Florida.

What I am hoping to hear from our guests' testimony today will focus on lessons learned from recent events and how to best move forward to ensure that America's consumers are protected. We have a steady drumbeat of high profile data security breaches in the last 6 months, and that has given many Americans, I would say most Americans, cause for concern.

My constituents are no different. Since I was first elected and came to Congress in January of this year, my office has received dozens of calls, letters and e-mails on this matter. In fact, it is probably the thing that has gotten the most attention and volume in my office.

One woman in Hollywood, Florida, wrote to me and said, "I am outraged that private companies can hold information about me without any national standards for whether or how they protect that information."

From another one of my constituents in Fort Lauderdale, she said, "It is time for Congress to give Americans meaningful identity theft protection, insist on strong security standards for information brokers with real penalties if they fail to keep my personal information secure."

The apparent ubiquity of these cases has clearly caused a great deal of alarm and also caused some confusion. What I would like to hear from the credit card company representatives today is for you to help clarify the difference between identity theft and credit card fraud, because there is clearly a difference. Both are very serious matters, but the credit card companies have developed effective consumer fraud protections to combat fraud and I think it is important to make that distinction.

Part of our challenge here is that many of the industry's guidelines and best practices that have been developed to protect consumer information have not been adopted by third party vendors and retailers; in other words, those in the payment stream. And I have always believed in personal responsibility, and this standard certainly applies to vendor and third party processors. Any company touching consumer data must be responsible and accountable for the way in which that data is managed.

Two of the largest security breaches announced this spring involved merchants that had maintained unnecessary credit card magnetic strip information, including card verification and replacement codes in violation of industry security rules. It has become quite clear to me that we need effective and consistent national standards for both how consumer data is managed and when consumers are notified about potential breaches.

We also have to make sure that we do not set fire alarms off for no reason. If there has been data that has been compromised but it is not necessarily a danger to the consumer, telling them absolutely everything that they think they need to know is not necessarily wise. Existing regulations are simply not sufficient, though, and I encourage my colleagues on both sides of the aisle, as Chairman Castle has, to build upon the industry's existing best practices and ensure that our consumers are protected.

Thank you. I yield back the balance of my time.

Chairwoman KELLY. Thank you.

Chairwoman Pryce?

Ms. PRYCE. Thank you, Madam Chairwoman. I appreciate the invitation to be here today.

The effects of data breach can be staggering to the American public. It is a problem that has to be addressed sooner or later. I just want to thank you for your interest in it, for you holding this hearing and commend Mr. Castle and Mr. Moore and Ms. Hooley and Mr. LaTourette for working together on a bipartisan basis to address this, and I look forward to moving legislation, as Mike said, sooner rather than later, because it is a problem of national significance, and I think the consumer confidence issues will begin to affect the economy if we do not do something soon.

So thank you so much for holding the hearing, Madam Chairwoman.

Chairwoman KELLY. Thank you very much.

Ms. Hooley?

Ms. HOOLEY. Thank you again for holding this hearing and for allowing me the opportunity to speak.

The topic of identity theft is one I have been working on for over 8 years, and the wave of data security breaches over the last few months has been one of the most troubling developments I have witnessed in that time.

Identity theft represents a fundamental threat to our e-commerce, to our overall economy and to our homeland security. No longer are we facing just "hobby hackers" looking to create a nuisance. Increasingly, these attacks are driven by skilled criminals. ID theft is huge business in this country.

Today, with Congressman LaTourette, we have introduced legislation that requires universal and timely notification to consumers when their personal, sensitive financial information is put at risk, as well as one free year of credit monitoring service when a breach places consumers at risk of identity theft.

I look forward to working with all of my colleagues on this committee and Ms. Pryce and Mr. Castle and Mr. Moore to pass the best possible legislation.

I am particularly concerned about the breach that occurred with CardSystems this May. The behavior of CardSystems was in direct

violation of agreements with MasterCard, Visa, and American Express. CardSystems placed 40 million consumers' financial accounts at risk. Now, while I recognize only 200,000 accounts were actually compromised—that is still a lot—in this case, I am not certain that consumer notification is enough.

Valuable financial information that was not rightfully owned or stored by CardSystems is what is at question here. I would like to applaud Visa and American Express for no longer doing business with CardSystems until they are sure that the problem has been resolved. And I am looking forward to seeing what CardSystems has done in the last few months.

Again, I thank you, and I look forward to this hearing and testimony from the panel. Thank you.

Chairwoman KELLY. Thank you.

Mr. Renzi?

Mr. RENZI. I thank the chairwoman for allowing me to be on the dais today and to participate.

I am a member of the Intelligence Committee and every morning have a chance to look and see the threat against the United States. There is no cybersystem security system available in the commercial marketplace that cannot be hacked. There are few systems that the government has that have not been hacked to date, but they necessarily are not in the commercial world. I say that to you in order to make the point that there is no perfect system.

I had a chance earlier this morning to meet with both the representatives from CardSystems and Visa. I am thankful that you both have expressed a good faith to meet privately and expeditiously within the next few days to see if you can work through the real facts, not those that just appeared in the paper that were just quoted, but work through some of the real facts and see if you can come up with solutions. I think that needs to happen.

We have over 100 Arizonans who work for CardSystems, whose jobs will be immediately lost, but a death knell will be put to CardSystems. Now, that has a chilling effect on those in the industry who have come forward and worked with investigators to show the truth and say, "Hey, look, this is what happened," rather than hide it.

So while some may applaud Visa and MasterCard for their actions, think about unintended consequences that may also occur.

So let me come back and say thank you to Visa and to CardSystems for giving me their word that they will meet in an expeditious manner, in a good faith manner to work through the facts that hopefully may work and lead to compromise. Either way, I am hopeful that there could be a solution that will be found that will protect both American consumers as well as those people who are an integral part of the credit card system here in America.

I thank the gentlelady for yielding me the time.

Chairwoman KELLY. Thank you.

Mr. Matheson?

Mr. MATHESON. Thank you, Madam Chairwoman.

And thank you, Ranking Member Gutierrez.

I am pleased the Oversight Subcommittee has scheduled this hearing regarding data security, and I am also pleased to be here

this morning to welcome David Watson, who is chairman of Merrick Bank, based in my home State of Utah.

I appreciate Mr. Watson taking the time and effort to travel to Washington to participate in this hearing regarding data security. I know that Merrick Bank and its employees have a good reputation with their clients and customers, and I appreciate their commitment to working with us on the credit card data issue.

The issue of data security is incredibly important to all of our constituents. Many people are concerned about the potential for credit card fraud and identity theft. I look forward to hearing the testimony of Merrick and all the other witnesses on the panel so we can learn more from their experiences and understand whether there are more reasonable steps, and I want to emphasize reasonable steps, that we can take to increase data security so that we can prevent theft of data and identity.

And with that, I will yield back my time to Madam Chairwoman.

Chairwoman KELLY. Thank you very much.

I am turning now to the panel.

We have a very distinguished panel with us: Mr. Joshua Peirez, who is the senior vice president and associate general counsel of the Legal Department of MasterCard; Mr. Steve Ruwe, executive vice president, Operations and Risk Management, Visa; Mr. Zyg Gorgol, senior vice president, Fraud Risk Management, American Express; Mr. Carlos Minetti, executive vice president, Cardmember Services, Discover Card; Mr. David B. Watson, chairman of the Merrick Bank; Mr. Mallory Duncan, general counsel of the National Retail Federation; Mr. John M. Perry, president and chief executive officer, CardSystems Solutions, Incorporated—and I have to say, sir, I am delighted to have you here, and I admire your courage for being here—and Mr. Evan Hendricks, editor and publisher of *Privacy Times*.

Mr. Peirez, we begin with you.

STATEMENT OF JOSHUA PEIREZ, SENIOR VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL, LAW DEPARTMENT, MASTERCARD INTERNATIONAL

Mr. PEIREZ. Good morning, Chairwoman Kelly, Ranking Member Gutierrez and members of the subcommittee. My name is Joshua Peirez, and I am a senior vice president and associate general counsel at MasterCard International, located in Purchase, New York.

It is my pleasure to discuss the important topic of fighting fraud and safeguarding financial information, and I commend the subcommittee for holding this important hearing.

MasterCard takes its obligation to safeguard financial information and protect consumers extremely seriously. This issue is a top priority at MasterCard where we have a team of experts devoted to working with law enforcement and maintaining the integrity and security of our payment systems. Our great success in protecting consumers and preventing fraud is due in part to the constant efforts we undertake to keep our networks secure. This is why our overall fraud rates are at an historic low, well below one-tenth of 1 percent of our volume.

MasterCard's information security program is comprehensive and we continually update it to ensure that it provides strong protection. MasterCard requires each of our customers and merchants and any third party acting on their behalf to safeguard cardholder information. In addition, MasterCard has a variety of consumer protection and antifraud tools.

Importantly, MasterCard has voluntarily implemented a zero liability rule. Under this rule, consumers will generally not be liable for any unauthorized use of their cards. In addition, MasterCard is focused on preventing unauthorized use in the first place through enhanced security features on the card, the MasterCard address verification service and our proprietary fraud reporting system which helps identify and prevent fraud from occurring in the first place.

We also offer services to our issuers and assist them in proactively identifying and stopping fraud.

I would now like to discuss the CardSystems situation. Several months ago, MasterCard and a few of our issuers noticed a small pattern of fraud. Working with our issuers, we traced the pattern of fraud to the acquirer, Merrick Bank, and then on to CardSystems, a third party processor the bank had hired. Once notified of the situation, CardSystems identified a script in its system designed to export cardholder data.

CardSystems then engaged a data security firm to conduct forensic analysis of its networks. The forensic investigation found that, first, CardSystems was storing transaction information on its system in violation of our rules. This was remedied in short order. Second, the investigation confirmed the presence of a malicious computer script on CardSystems systems, along with other serious security vulnerabilities. And, third, there was evidence that some cardholder data had been compromised.

Based on the findings, we believe approximately 68,000 different MasterCard accounts and well over 100,000 accounts of other brands were exported from the CardSystems database. The matter is under investigation by the FBI.

Upon learning this information, we demanded that we be provided with the account numbers impacted as soon as possible, and we received the file on June 16th. We notified the banks that had issued the impacted accounts beginning the very next day and are continuing to monitor the potentially affected accounts with those banks.

Given the circumstances of this case, MasterCard made the decision that a public disclosure of the event was warranted. Thus, on June 17th, we issued a press release to notify the public of the situation at CardSystems.

I would like to stress that we provided broad public disclosure because it was the right thing to do, even though we had no legal obligation to do so. We continue to closely monitor CardSystems' efforts to cure their deficiencies and have given them only until the end of August to do so.

Let me now turn to a brief discussion of possible legislative measures to help address the issue. MasterCard strongly supports the legislative efforts to enact uniform national standards and believes it is critical that any legislative solution: one, strengthen

criminal penalties to be in line with the severity of these crimes; two, provide notification to consumers in appropriate circumstances; and, three, establish strong data protection requirements for entities not already covered by the Gramm-Leach-Bliley Act.

MasterCard looks forward to working with you as you tackle these important issues, and I would be pleased to answer any questions you may have.

[The prepared statement of Mr. Peirez can be found on page 98 of the appendix.]

Chairwoman KELLY. Thank you very much.

Mr. Ruwe?

STATEMENT OF STEVE RUWE, EXECUTIVE VICE PRESIDENT, OPERATIONS AND RISK MANAGEMENT, VISA U.S.A. INC.

Mr. RUWE. Chairwoman Kelly and members of the subcommittee, my name is Steve Ruwe. I am the executive vice president of Operations and Risk Management for Visa U.S.A., Incorporated. Visa appreciates the opportunity to appear at today's hearing on the issue of 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 initiatives for protecting cardholder information and preventing fraud.

Cardholder security is never an afterthought at Visa. For Visa, it is 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 protecting consumers from fraud includes Visa's zero liability policy, which protects Visa cardholders from any liability for fraudulent purposes.

Because the financial institutions that are Visa members do not charge their cardholder customers for fraudulent transactions, those members absorb most of the cost from fraudulent transactions.

Visa has implemented a comprehensive and aggressive security program known as the Cardholder Information Security Program, CISP, which applies to all entities that store, process, transmit, or hold Visa cardholder data. Visa also provides sophisticated neural networks that flag unusual spending patterns for fraud that enable our members to block authorization transactions where fraud is suspected.

Only yesterday, Visa announced a new nationwide data security education campaign that will involve both the payments industry and merchants in the fight to protect cardholder information. Visa believes that all parties who participate in the payment system share responsibility to protect cardholder data.

When cardholder information is compromised, Visa notifies the issuing financial institution and puts the affected card numbers on a special monitoring status. Visa also uses an array of other security measures that are described in my written statement to prevent particular fraudulent transactions. As a result of these strong security measures, fraud within the Visa system is at an all-time low of 5 cents for every $100 worth of transactions.

Visa was recently informed by payment processor, CardSystems Solutions, Incorporated, CSSI, about an unauthorized intrusion into CSSI's computer system. Visa immediately worked with the processor, law enforcement, and affected member institutions to prevent card-related fraud and respected law enforcement protocol to keep the information about the investigation confidential.

Visa notified all of the potentially affected card issuing institutions and provided them with the necessary information so that they could monitor the accounts and, if necessary, advise customers to check their statements or cancel or reissue cards to their customers. The card-issuing institutions that are members of the Visa system have the direct responsibility and relationship with their customers, and because of Visa's zero liability policy for cardholders, bear most of the financial loss if fraud occurs. Visa institutions can best determine the appropriate action for each customer that might have been affected.

We have determined that about 22 million Visa card numbers from the CSSI database were put at risk. In many of these cases, CSSI, by its own admission, knowingly and improperly retained magnetic stripe information, which was a clear violation of the cardholder information security program.

Because of CSSI's failure to follow Visa's security requirements, Visa is terminating CSSI's ability to act as a processor for Visa members. Protecting our cardholders was, and remains, Visa's primary goal in responding to this incident.

Significantly, the information retained by CSSI did not include the cardholders' date of birth, address, Social Security number, or driver's license number. Visa believes that the information involved in this incident cannot be used to commit identity theft—identity fraud against an individual in which a criminal opens a new account in the individual's name.

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

[The prepared statement of Mr. Ruwe can be found on page 119 of the appendix.]

Chairwoman KELLY. Thank you very much.

I wanted to step into a bit of housekeeping. The two boxes at the end of the table indicate green, yellow, and red lights. The green light means you have 5 minutes, the yellow means you have one minute to sum up, the red light means that it is time to end your testimony.

I just simply wanted all of you, in case you have not testified before Congress before, to understand how that system works and if you wondered what those lights were doing.

Mr. Gorgol?

STATEMENT OF ZYG GORGOL, SENIOR VICE PRESIDENT, FRAUD RISK MANAGEMENT, AMERICAN EXPRESS

Mr. GORGOL. Chairwoman Kelly, Ranking Member Gutierrez, members of the subcommittee, my name is Zyg Gorgol, and I am a senior vice president of Fraud Risk Management at American Express.

My responsibility is to protect our customers by preventing fraud or identifying and minimizing it as quickly as possible. I appreciate

the opportunity to testify today about the recent data security breach at CardSystems Solutions and its impact on American Express cardmembers.

We view this breach with great concern and have taken steps to protect any cardmembers who may have been affected by it.

I would like to highlight a few key points today, so the complete body of my comments have been submitted to the committee.

First, I would like to discuss the Payment Card Industry Data Security Standards. They provide an industry-wide approach to safeguarding charge and credit card customer data. These PCI standards were developed by a cross-industry working group that included American Express and the other major card networks.

American Express fully endorses these standards as an appropriate industry baseline for data security in the payments industry.

Let me now specifically discuss CardSystems. As background, CardSystems Solutions processes less than 1 percent of American Express card transactions. Upon learning of the breach at CardSystems, we began an investigation to determine any impacts on American Express cardmembers. We also put additional security and fraud prevention measures in place for all American Express card accounts that were on their database. We are continuing to closely monitor these accounts for any suspicious activity on an ongoing basis.

Based upon our current analysis, we have determined the following: 1.6 million American Express card accounts were stored on the database; information relating to approximately 12,000 American Express card accounts appears to have been acquired by unauthorized persons. Although the information relating to these 12,000 accounts included the card account number and expiration data, it did not include any personally identifiable information, such as name, address or Social Security number.

While we have been closely monitoring these accounts, we have not detected any increased incidences of fraud on these 12,000 accounts, nor have we detected any increased incidence of fraud across the total number of accounts that were on the CardSystems database. We are continuing to monitor all of these accounts for any suspicious activity every day, and we continue to investigate where the criminals accessed any other American Express card accounts.

It is important to know that American Express employs sophisticated monitoring systems and controls to detect and prevent fraudulent activity. Historically, this has been an area of emphasis for American Express. Over the last several years, we have invested tens of millions of dollars to enhance our fraud prevention capability to better protect cardmembers.

If fraudulent charges are placed on an American Express card account, we stand behind our cardmembers. American Express cardmembers are not held liable for fraudulent charges.

Finally, we believe there are some tangible steps that can be taken to better protect consumers. Most importantly, we recommend that Congress extend Gramm-Leach-Bliley-like safeguard standards to those companies involved in processing card payments that are not currently subject to those safeguards today.

Sensitive customer information should be consistently protected as it passes throughout the payment card transaction cycle.

In conclusion, I want to assure the subcommittee that American Express is strongly committed to protecting the security of our cardmembers' personal information. It is clear that recent events have raised the public's concern regarding security of their personal information. We share this concern and are constantly working to protect the security of our cardmembers' information so that when a customer makes a transaction they have a confidence that it will occur in a safe and secure manner.

We appreciate the opportunity to share our views on this issue and look forward to working with you and members of the Financial Services Committee.

This concludes my testimony. I would be happy to answer any questions you may have.

[The prepared statement of Mr. Gorgol can be found on page 66 of the appendix.]

Chairwoman KELLY. Thank you very much.

Mr. Minetti?

STATEMENT OF CARLOS MINETTI, EXECUTIVE VICE PRESIDENT, CARDMEMBER SERVICES, DISCOVER CARD

Mr. MINETTI. Madam Chairwoman and members of the subcommittee, thank you for inviting Discover Financial Services to share our views on the issue of data security breaches affecting credit card information.

My name is Carlos Minetti, and I am responsible for operations and risk management at Discover. This includes oversight of Discover's information security and antifraud efforts. Discover works very hard every day to prevent customer information from falling in the hands of individuals who would hope to use it for criminal purposes, like account fraud or identity theft.

Discover Bank, the issuer of Discover cards, is a financial institution subject to Gramm-Leach-Bliley information security standards and the interagency guidance on security breach response programs. The FDIC examines Discover Bank for compliance with those standards, and our data security program is designed to perform with them.

At Discover, we have a number of different fraud and identity theft prevention programs, which are described in my written statement. In fact, in 2005, "Identity Fraud Safety Scorecard for Credit Card Issuers," conducted by Javelin Strategy and Research, ranked Discover as number one in overall card safety features.

Today, I will focus on our response initiatives. Because we operate both a large merchant network and issue the Discover Card, we are often able to learn about computer hacking and other signs of data compromises when they first occur. In fact, Discover was the first network to uncover evidence of data compromises in many of the recently publicized security breaches involving large merchants and payment processors.

Upon learning of a data security breach that may affect Discover Cardmembers, such as the CardSystems Solutions incident, we immediately commence an investigation. We first ascertain the type

of information involved to determine whether the data could be used to commit identity theft or otherwise harm the consumers.

We also identify the specific accounts that were affected, monitor those accounts, and take further action if necessary, such as contacting our customer or closing the accounts.

Where the breach occurs at merchants or processors, we must rely on information from those companies. We work with them and with their party of forensic investigators to validate the breach and its impact on Discover Cardmembers. We also work with other card networks when their account data is affected. It is critically important for all these parties to cooperate fully in the investigative process.

Discover carefully weighs all relevant facts and impacts on our customers to determine the proper course of action. If we determine that a breach is likely to harm our customers, we notify them in accordance with the Interagency Guidelines and the requirements of State laws. We also take further action as may be necessary to prevent harm, such as further monitoring or closing the accounts. We coordinate our efforts with the FDIC and with law enforcement personnel who may be investigating the incident.

As the subcommittee is aware, not every data breach resulted in any theft of consumer exposure to substantial costs and time-consuming efforts to remedy misuse of personal information. As a result, it is often not necessary to immediately notify consumers, close accounts, provide credit report monitoring, or put fraud alerts in consumers files.

Discover Cardmembers are not responsible for unauthorized charges, and our 24–7 customer service allows to quickly remove the fraudulent charges from their account. Industry resistance to across-the-board up-front notification, card reissuance, and other requirements is not based on the cost involved.

Given the fact that potential fraud-related losses are incurred by credit card issuers and not by the consumers and can quickly eclipse the cost of notification and/or card reissuance, the customer notification/reissuance is generally not the driving factor for decisions about how best to react in a given situation.

Our investigation of the CardSystems Solutions security breach is ongoing. This breach is very troubling and should never have occurred. Based on what we know today, it does not appear that Discover Cardmembers were exposed to a risk of identity theft, because the Discover data was limited to purchase transaction information.

While the CardSystems breach did involve a loss of Discover data that could be used to commit account fraud, Discover Cardmembers will not experience financial loss as a result of this incident.

As the committee considers the need for legislation, addressing information security and identity theft, we hope you will consider our recommendations. First, a single national standard for responding to security breaches affecting personal information is appropriate. Second, the Interagency Guidelines coupled with onsite compliance examinations establishes an effective and proper regime for information held by the national institutions. It also provides regulators with the flexibility they need to adjust breach response standards.

Finally, when a data breach affecting credit card information occurs, notification is best handled by the card issuer, not the entity whose security was breached. An entity whose security was compromised must cooperate fully in investigating the incident and preventing further fraud, but it should not be charged with contacting credit card customers who may have been affected. A single notice is the best way to protect credit card users, and card users are in the best position to determine whether and when that notice is appropriate.

We appreciate the opportunity to discuss information security issues, and we would be pleased to provide further information that would be useful to the subcommittee.

[The prepared statement of Mr. Minetti can be found on page 85 of the appendix.]

Chairwoman KELLY. Thank you.

Mr. Watson?

STATEMENT OF DAVID WATSON, CHAIRMAN, MERRICK BANK

Mr. WATSON. Madam Chairwoman, ranking member, and members of the subcommittee, thank you for inviting me to testify today. My name is David Watson.

As a cardholder myself and as chairman of a card-issuing bank, I commend this committee for its diligence and its interest in formulating good public policy on credit and security—a topic of importance to virtually every American.

Merrick Bank is a Utah financial institution, subject to regulation and annual examination by the FDIC and the Utah Department of Financial Institutions. We issue credit cards to accountholders, and we make payments of processed credit card transactions to merchants.

Credit card and account holder security is a fundamental principle of our business; it has to be.

First, a little bit about the credit card payment process and then Merrick's relationship with CardSystems.

To most consumers, the credit card system seems marvelously simple and dependable but behind the scenes multiple players and a sophisticated series of steps are triggered in each of the millions of daily credit card transactions. Each step must be performed with precision, for the integrity and security of the process is only strong when the performance of each party is strong.

The merchant initiates the transaction, the processor authorizes the transaction and sends the notice for payment to the cardholder's bank and then ensures that the merchant is paid. The paying bank is then reimbursed by the card issuer's bank through the Visa and MasterCard settlement networks. All of this is conducted according to rules imposed by the individual card associations.

Like many other banks, Merrick Bank makes payment to merchants who use CardSystems for processing. Before September 2003, we did not have any significant business contacts with CardSystems, although they were a known entity in the card processing field.

Following 2003 discussions concerning the transfer of certain Provident Bank merchant contracts to Merrick, we advised CardSystems that we could not consider participating in any proc-

essing unless and until CardSystems became compliant with the Customer Identification Security Program, which you have heard is the CISP Program, and the Visa Data Security Accreditation Program.

CardSystems then engaged Cable & Wireless, an auditor from the Visa group auditor list, to conduct the CISP assessment. Cable & Wireless was selected by CardSystems, paid by CardSystems, and the audit report that resulted was sent to Visa. In June 2004, Visa informed CardSystems that it was just approved, and CardSystems so notified Merrick Bank.

We then successfully took over most of Provident Bank's merchant payment contracts effective September 30, 2004. From that point to May 2005, Merrick's payments for the transactions presented by CardSystems proceeded routinely.

After initial inquiries from MasterCard regarding potential fraud activity, on May 22, 2005, CardSystems identified a security breach in its operation and on May 23rd, contacted the FBI. On May 25th, CardSystems contacted Merrick and advised us of a possible intrusion and export of cardholder data at CardSystems.

Merrick reviewed this information and notified Visa and MasterCard of the potential security breach. On May 27, 2005, with the approval of MasterCard and Visa, Merrick engaged Ubizen, a well known forensic IT audit firm to thoroughly investigate the breach at CardSystems, and Ubizen began an onsite examination of CardSystems at its Tucson facility on May 31, 2005. We also sent our chief security officer and our senior network engineer to the CardSystems site to investigate the issue and see that immediate action was taken to prevent any further breach.

The Ubizen audit identified two issues at CardSystems. First, CardSystems had retained certain transaction data on their system in violation of association procedures. Ubizen reports this data retention practice had been followed by CardSystems since 1998, even though it was inconsistent with CISP standards.

This was not identified by the Cable & Wireless report in the 2004 Visa certification process.

Second, Ubizen identified certain issues with CardSystems servers and software, which were compromised by the intruding party. Again, unfortunately, the Cable & Wireless report did not make any mention of these vulnerabilities.

Merrick Bank, Ubizen, CardSystems, Visa, and MasterCard have all been aggressively working together to see that the issues permitting the breach are corrected and that CardSystems' data environment is fully secured. Visa and MasterCard have identified the cardholders whom they believe may have been compromised and have sent notice to the issuing banks of the potentially affected cardholders. This was accomplished by June 17th.

Merrick is taking additional steps. We are preparing a contingency plan to assure our merchants are serviced without disruption in a secure environment. In addition, in consultation with security and data experts, Merrick is developing its own set of requirements to assure card processor compliance with all applicable card association standards.

I want to conclude by reiterating our absolute commitment to data security. We are very closely monitoring for unusual activity

the accounts of any affected cardholders. While we deeply regret any impact that this breach has had on consumers, we understand this presents all of us with an opportunity to help our industry improve our systems and processes and thereby better protect consumers' interests.

I want to again commend this committee for its hard work and good work to formulate sound public policy that will assist us in achieving this goal. Thank you.

[The prepared statement of Mr. Watson can be found on page 127 of the appendix.]

Chairwoman KELLY. Thank you.

Mr. Duncan?

STATEMENT OF MALLORY DUNCAN, GENERAL COUNSEL, NATIONAL RETAIL FEDERATION

Mr. DUNCAN. Thank you, Madam Chairwoman. I am Mallory Duncan, senior vice president and general counsel for the National Retail Federation. The NRF is the world's largest retail association with membership that comprises all retail formats and channels of commerce. We appreciate the opportunity to testify here today.

There has been a substantial increase in the reported incidence of identity theft. Federal Trade Commission data indicates that identity theft complaints increased 8-fold to nearly 250,000 between 2000 and 2004. Recently, an FTC survey estimated 10 million people experienced identity theft within the past year. Even larger numbers have been published elsewhere.

The reported numbers are rising, but we do not know how much of that is a real increase as opposed to increased awareness of those reporting; versus mischaracterization of the problem.

As striking as these figures are, it is important to recognize that the fraud that they reflect comprises a variety of activities, not all of which are true identity theft.

I suggest we look at this issue broadly. We have to ask, how do businesses know who we are? Relatively few of us reside in communities with bankers and shopkeepers who have known us since birth. Instead, proof of our identity has shifted from being something others vouch for to something that is inferred: from identifiers such as driver's license and Social Security numbers, and quick recall of personally related facts, such as date of birth, mother's maiden name, and office telephone numbers.

True identity theft occurs when someone appropriates identifying data for the purpose of secretly committing fraud. The thief may attempt to open credit and checking accounts, purchase a car, even buy a condominium using the victim's excellent credit history. So long as the thief makes payments, it might be years before anyone discovers the fraud. On the other hand, the thieves may decide to stiff the creditors, potentially ruining the victim's credit report. In that case, it could takes months or years for victims to recover their good name. Worse, if not apprehended, there is the possibility the thieves will strike again.

In contrast, much of what is commonly referred to as identity theft is in fact credit card fraud. While it can be a problem for those affected, credit card fraud is much closer to a serious nuisance than it is the horror of identity theft. Equally important,

Congress long ago approved many of the tools needed for its correction. Under the Fair Credit Billing Act, the consumer may challenge charges and be held harmless for the loss. Either the retailer or the card issuer bears the cost of the loss.

With this distinction in mind, it is clear that the incidence of identity theft is, fortunately, considerably different than some of the numbers that have been cited. Even if one accepts the 10 million estimate by the FTC, it turns out that two-thirds of that is not truly identity theft.

Now, I go into this distinction because the remedies for these two frauds are quite different. Credit card fraud is usually is an on-off event. Once discovered, credit card fraud is relatively simple to stop by closing the account and reopening a new account number—a pain, but it can be stopped.

On the other hand, when identity theft occurs, it is not a simple matter to change an individual's Social Security number, date of birth, or mother's maiden name. If society has limited resources that it can devote to fighting crime, then we ought to tilt toward using those resources to help consumers faced with the more serious consequences.

Indeed, this committee recently established many new protections for identity theft victims with the FACT Act. Now, although identity theft grabbed the headlines, retailers have devoted considerable attention to reducing the incidence of credit card fraud as well.

Several retailers issue their own cards. They want to protect the integrity of their cards and essentially treat all cards with the same level of security. Currently, merchants are coming online with the Visa and MasterCard new security program. Initially developed for your Internet transactions, the card associations are extending these to all channels of commerce.

The FTC recently entered into a proposed settlement with BJ's Wholesale Club as a result of system attacks in 2003. Retailers are paying particularly close attention to the requirements of that settlement. And when there are losses, they are typically borne by the retailers, yet another incentive for us to want to reduce the incidence of both types of fraud.

In closing, identity theft is a fairly focused but especially pernicious form of fraud. Proof of identity has become a more elusive quality at the very moment that our society is investing greater amounts of trust in its veracity.

Viewed from a distance, our credit system is marvelous. Families receive a meal in exchange for a swipe of plastic. Individuals secure home financing from bankers they have never met. These benefits flow not from credit cards but from the trust our society invests in the identities of persons seeking credit. If we are to preserve these benefits, society must crack down on those who would abuse that trust by appropriating the core elements of identity.

With the passage of the FACT Act, Congress has begun to provide tools to those who have been victimized. It should now provide incentives to ferret out and prosecute those who make use of those tools necessary.

Thank you for the opportunity to appear today. I will take your questions.

[The prepared statement of Mr. Duncan can be found on page 54 of the appendix.]

Chairwoman KELLY. Thank you.

Mr. Perry?

STATEMENT OF JOHN M. PERRY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CARDSYSTEMS SOLUTIONS, INC.

Mr. PERRY. Good morning, Madam Chairwoman and members of the subcommittee. Thank you for inviting CardSystems to appear before you today. We appreciate the opportunity to address the issue of data security and more specifically the recent security attacks perpetrated against us.

First and foremost, we truly regret this occurrence of data theft. We have readily acknowledged our error and continue to work nontop to ensure that we do not become a target of another breach.

I had planned to provide you with some prepared remarks today discussing policy implications of the security incident hat occurred at our company, and I had an opportunity to discuss that important issue with some of your staff yesterday. But today, a small company with 115 employees, in Atlanta and Tucson, is facing imminent extinction. That concerns me greatly, not just because of how it will impact our company but because how it will impact 110,000 merchants who rely on CardSystems to process their transactions.

If CardSystems is forced to close its doors, many of these merchants will be unable to process credit card transactions for days or even weeks. Signing up with a new processor is not merely as simple as changing from one phone company to another. It can cause significant disruptions to a business' operation. Moreover, I am concerned about the signal that our experience sends to other payment card processors and businesses, one of which undoubtedly faces a similar security incident in the future.

We came forward in May to report this incident to law enforcement officials and our sponsor bank. As a result of coming forward with this important information, CardSystems is being driven out of business. Our experience should send a troubling message to policy makers. Other companies will have less incentive to come forward in the future when similar breaches will undoubtedly occur, knowing the potentially catastrophic effect that they could have on their businesses as well.

We are still learning from the ongoing investigation but we do know this: That the attack on our system was very sophisticated. Based on the forensic investigation, we know of only one confirmed instance of which data was exported and that is the May 22nd incident that has brought us here today. I am relieved to report that this breach, to our knowledge, has not resulted in identity theft. By design, information is fragmented among different players in the payment card industry. This means processors like CardSystems do not have access to complete information, such as Social Security numbers, which could greatly facilitate identity theft.

Additionally, this breach has not, to our knowledge, resulted in credit card fraud. Make no mistake, exposure of information about one card is too many. We will not be satisfied until we are con-

fident that everything that can be done has been done to prevent this from ever happening again.

Turning to the issue of security compliance, all businesses that handle cardholder data are directed by the payment card networks to follow rigorous security standards. CardSystems was audited and certified in the late fall of 2003 by a qualified Visa security assessor. More recently, Via and MasterCard have developed the payment card industry, or PCI, data security standard, which has been adopted by all the card networks. We have hired an independent security auditor who has reviewed our systems and has affirmed that we will be PCI compliant by the end of the month.

We are also pleased to hear today that Visa has agreed this morning to meet and discuss and, I am confident, to resolve our differences. As MasterCard has just noted, I am sure that we will complete the necessary work to satisfy all requirements for continuing our work as processors by August 31st.

We appreciate the opportunity to participate in this hearing, and we welcome the chance to address any questions from the subcommittee. Thank you.

[The prepared statement of Mr. Perry can be found on page 105 of the appendix.]

Chairwoman KELLY. Thank you.

Mr. Hendricks?

STATEMENT OF EVAN HENDRICKS, EDITOR AND PUBLISHER, PRIVACY TIMES

Mr. HENDRICKS. Thank you, Chairwoman Kelly, Ranking Member Gutierrez.

This is my first time back since the 2003 FACT debates. That year inspired me to write my book, "Credit Scores and Credit Reports," which spends a lot of time trying to explain to consumers what to do in situations like this. It also has a chapter dedicated to Congress' and this committee's work, which was an exciting and productive year, I think, for all of us.

I think it is also worth pointing out that this committee, your subcommittee, was the first one to hold a hearing on a data breach involving a credit card processor, I think it was April 2003. So you continue to be out in front of this issue, and look at the response you get by shining the spotlight. I think it is very commendable.

I think there are several lessons from this event. One is that some companies will not have adequate security unless they are forced to. They will continue to treat security as an afterthought. I think you used to say that privacy is good for consumers and good for business. I think we have elevated to the point now where privacy and security is not only good, it is essential, and that you see by blowing it on privacy and security, that there are serious economic repercussions.

Here a company is faced with an enforcement action that could close them down or seriously reduce them in size. It would have been good to have considered not to keep personal information that you were not supposed to keep in the first place and if you were, to encrypt it so it would be rendered useless with robust encryption. I hope other companies will learn the lesson that in ignoring privacy and security, you do so at your own risk.

I think the other thing that we have to remember is the consumer. These incidents impose real costs and hardships on consumers. I have already heard from a few who did not receive any notice of this event, went into the retailer and found out that their account had been flagged and were unable to make purchases. Some were accompanied by friends or by business associates.

Other people, consumers, have called to try and find out, "Has my information been compromised?" Some credit card companies were fairly responsive. Others did not have a clue what to tell people, and so this again contributes to the anxiety. If we are going to have a system where notice is not going to be required for every little event, then it is incumbent upon organizations to have a mechanism in place to inform people who are trying to find out what is going on.

The other lesson from this is some companies will not notify consumers unless they have to. Some companies will make the judgment that there is no real harm to people. And the problem with that is that if you get a credit card number in this sophisticated hack, the sophisticated hackers and identity thieves can use a credit card number as leverage to get a Social Security number through pretext and other means. We need to stop treating the lowest priority as the consumer because the consumer is the basis for this entire credit card system.

If we look at the breaches that we have had this year, ChoicePoint, Bank of America, CitiFinancial, 3.9 million Social Security numbers about to go out the door and what do they do, they call UPS. They are not encrypted, and the information is lost by UPS. And now with CardSystems and potentially 40 million, the number of Americans that are potentially exposed to these security breaches equals the number of Americans that originally signed up for the "Do Not Call" list. So it is sort of an eerie mirror of the privacy issue.

The other thing that shows the inadequacy is what is not known. I mean, there are more things that we do not know about what happened with this data, how it went out, who it went to, and, again, there is no transparency, there is no reporting to the public.

The lack of encryption is very troubling. We want to encourage encryption, but we also want to keep in mind that encryption by itself is never going to solve the problem. It is a multifaceted problem and encryption has to be robust and meet certain standards. Just because you call it encrypted does not mean that it is adequately protected in this day and age.

The biggest threat here, I think, is the one to our society, is the lack of confidence that is going to entail from all of these events. If you look at each event and then total them up, as a consumer you do not think there is anyone out there looking for your data and that lack of confidence could have enormous implications, just as it is having for the Cingular company. If there is falling confidence in our credit card system, the numbers on that could be really scary.

And think what Congress did to build confidence in the credit card system. Congress, you like to beat up on yourselves, all the members like to joke about yourselves, but give yourselves credit. You passed the Fair Credit Billing Act a couple decades ago to

make sure consumers were protected, to put confidence in the system so that people were not going to lose their finances if something went wrong with their credit card. That is the kind of protection we need in terms of people's data. That is how this has migrated.

Chairwoman KELLY. Mr. Hendricks, will you please sum up?

Mr. HENDRICKS. Yes. In closing, I would say this is a very multifaceted problem. I urge the committee to be as comprehensive as possible in addressing it and to look at the key moment, the reason thieves steal identities is because the credit report continues to be disclosed when the thief applies for credit in your name.

Thank you, and I am sorry to have gone over.

[The prepared statement of Mr. Hendricks can be found on page 78 of the appendix.]

Chairwoman KELLY. Thank you very much.

I would like to ask a question about a company that is not represented here. I would like to ask Visa, Cable & Wireless security was part of your approved auditor list and CardSystems picked Cable & Wireless from that list.

I would like to know how Visa certified Cable & Wireless, and I would like to know since Cable & Wireless has been bought by an international company, now it is called the SAVVIS Company apparently, I would like to know if that SAVVIS Company has been tasked to do a better job than Cable & Wireless.

What can you tell me, Mr. Ruwe?

Mr. RUWE. Yes. Cable & Wireless is one of a number of vendors that are approved by Visa and/or MasterCard to perform assessments in this environment. As you said, the processor in this case selects from a list of those assessors and contracts with them to conduct the assessment and provide the assessment results to Visa or MasterCard or whoever it is going to.

In the case of Cable & Wireless, they are now, as you mentioned, SAVVIS. Visa has asked SAVVIS to explain how there could be such a discrepancy in the report of compliance between what was reported to Visa in reality. We have temporarily suspended SAVVIS from being able to do any more security assessments, and we have asked them to revalidate the last "X" number of assessments they have conducted.

So the investigation as to what happened in terms of the discrepancy that was very large of what was the case at CSSI versus what was in the report provided to Visa on behalf of CSSI is still under investigation.

Chairwoman KELLY. Mr. Ruwe, and I would ask you too, Mr. Peirez, how do you set up the goals that you expect the auditing companies to meet? What standards are you applying before you put them on your list?

Mr. Peirez?

Mr. PEIREZ. Thank you, Madam Chairwoman.

Well, obviously at this point in time, a lot of this information is new to us as well, in terms of what happened in this particular instance, as we were not privy to this report.

That being said, we obviously are looking at the measures in order to have auditors who are effective, who know what they are doing, and who can give accurate reports. We look for auditors who

follow standard auditing practices and look for them to issue reports that are within those guidelines. There are many standards out there for best practices of auditors, and that is what we look at.

Chairwoman KELLY. So you use whatever the standards are that are in the industry but do not have separated standards of your own.

Mr. Ruwe?

Mr. RUWE. There are in the case of assessors that Visa uses, and I believe this is true now of MasterCard, perhaps it was not at that time, there is a set of documentation that the assessor is given as a minimum that could be provided to the committee if they would like to see it, a minimum of standards that define and delineate and categorize the things that they have to check within that environment. That is as a minimum.

Beyond that, as a processor, assessor in this space, these companies have proven themselves to be viable and capable of doing this work, otherwise they would not be on the list.

So there is an actual process that is defined that they have to go through as a minimum for the PCI Program, and then beyond that they have their own additional assessments that they conduct.

Chairwoman KELLY. Mr. Gorgol, Mr. Minetti, I would like to have you please chime in on this. Tell me what your standards are.

Mr. GORGOL. At American Express—

Chairwoman KELLY. Mr. Gorgol, I am sorry—

Mr. GORGOL. Sorry.

Chairwoman KELLY. Thank you.

Mr. GORGOL. At American Express, we have the data standards in our contract with companies like CardSystems, the processors, and there are consequences to not meeting those standards. And you can see recently that those consequences do have teeth. But we also rely on the industry, and we would expect processors to draw from the industry and bring in professional help to make sure that they are meeting that contractual obligation.

Chairwoman KELLY. Mr. Minetti?

Mr. MINETTI. Our requirements are also outlined in our contracts. In addition to that, when we select the vendors we conduct an RFP, a request for proposal. I am not familiar with the criteria in the RFP, but it was a competitive process and we selected the top vendors of that list.

Chairwoman KELLY. Perhaps, Mr. Minetti, you could—

Mr. MINETTI. I can provide it.

Chairwoman KELLY. —advise the committee in writing. It is something of concern because if you all rely on auditors, then it is important that reliance is a correct one.

Mr. MINETTI. And I will be happy to provide you with a written statement that outlines the criteria.

Chairwoman KELLY. Fine. Thank you very much. My time is up.

Mr. Gutierrez?

Mr. GUTIERREZ. Thank you.

Well, first, I want to commend Mr. Ruwe and Visa for being a leader in the industry and initiating heightened security which became the PCI standard for the industry, and I commend the other companies for working to make this an industry standard. I think

it is a step in the right direction in terms of securing data of the public, which Mr. Hendricks so clearly elaborated we should be most focused on here at this hearing.

And I think, Madam Chairwoman, I think your questions about the audits are excellent, and we should examine who performs these audits and what standards are used and what the best practices are for these audits that are used by Visa and MasterCard and all of the other credit issuing companies, because if you have a bad audit, they all have bad information and our checks and balances, I think, are all out of whack.

So I think it is a great place. I am happy that you went in that direction, and I am going to be asking Visa to put in writing, if they would for me, just what happens at the audit, what flaws they saw in the audit and what actions they took with the auditor after they saw the vulnerabilities of the audit.

I would like to say also that it seems to me that we have a very, very serious problem here, because trying to set aside the issues of the processor and the credit card issuing companies, I mean, as I read these prepared statements and I look back and they say that there were—and I would like to ask Mr. Perry about this—your testimony has indicated that the data relating 239 accounts was transferred out of your system.

And this looks as though this number—239,000, thank you very much—this look as though this number can be tracked to only one day of transfer activity since the hacker software was on your system since September of 2004 through May of this year and was designed to download data every 4 days. That is in your testimony that he actually entered your system—he or she, they actually entered your system in September.

So it just seems extremely unlikely that a hacker, a sophisticated hacker would enter your system in, say, September, October, November, December, January, February, March, April and finally in May decide to download this information. And Merrick Bank did an audit, a forensic audit and their auditor suspects and found information that your system was probably already vulnerable as early as April of 2004.

Do you have any other information, I mean, is it your testimony that the only information that you have is of the 239,000 names downloaded that one day, that was the only security breach at CardSystems?

Mr. PERRY. Mr. Gutierrez, regarding that question, the only export of data that has actually been confirmed where it is possible to actually describe the number of accounts that were exported from the system was the security incident that occurred on May the 22nd, Sunday afternoon, I believe, when I heard about it.

Mr. GUTIERREZ. Well, it just seems rather unlikely and given the forensic information that Merrick Bank put together in saying that your system was probably already hacked into and that you were vulnerable much earlier than that, that a hacker would just wait that long to download information on one particular day, which only tells us that we need to be more secure, because even in your testimony and other people's testimony, you were vulnerable for months if not for over a year before you found out that somebody actually downloaded some information.

And, secondly, the information that you held, why did you hold information that clearly was established in the contract, at least with MasterCard, in the information I have received, with MasterCard and Visa that you were not supposed to have in your system?

Mr. PERRY. Mr. Gutierrez, the data that was actually exported on that day that we notified the FBI and Merrick about was from a database that was used primarily for research purposes.

Mr. GUTIERREZ. I guess my question is, why did you have the data in your system if your contract with MasterCard and Visa, I do not know about the other two companies, but at least with those two companies they said, "This is part of our contract. We do not want you to have this information."

Mr. PERRY. Mr. Gutierrez, we have stated that we were in error by keeping that data. That data was specifically designed to provide customer service to the merchants that might have had a transaction that did not properly execute, it did not properly process, and the individuals in that case that managed that database believed it enhanced customer service to provide the merchants with the information they would need to conduct their business.

Chairwoman KELLY. Thank you.

We turn to Mr. Garrett.

Mr. GARRETT. Thank you.

I appreciate Mr. Watson's opening comments about the simplicity of the system and how the average consumer just deals with it in an easy manner. From a government point of view, I can go to a local government agency, whatever it is, try to transact some sort of action with the government, it may take me some hours or days or even weeks to get some sort of response from the government, but I can go across the country or across the world and just open my wallet and bring out my credit card and given it them and literally within seconds or a minute or 2 they know who I am and I can get into a hotel or, as you say, have dinner or something like that.

So it is an amazing ability that we have developed or that you all have developed, and I guess the track record has been fairly good in the scheme of things, and unfortunately we come to this point in time when it occurs as it does here, but I think I want to commend that it has been able to move the economy as it has in the system that we have had so far.

The concern we have is whether we need to be taking additional actions right now or, as I see from one of the charts that we have here, literally the litany of regulations that applies to the various players, whether it is the issuing banks, the merchants, the ISO's, the card services, and it goes from the Federal banking laws, the FACT Act, the FTC safeguard rules, the bank regulators acts and so on. So we have a lot on the books already, and I know some of you who are before us are involved in the regulatory side of the game.

Let me turn first to Mr. Perry then on that regard. Someone else had made mention, I believe, earlier with regard to Gramm-Leach-Bliley and how that applies here or it does not apply here. Your understanding as to whether that applies to you or not?

Mr. PERRY. Mr. Garrett, we are currently conformed to the regulations and rules of the card associations who set before us, including Visa and MasterCard, who set before us the rules on how we process timeframes, etc.

Mr. GARRETT. Okay. If anyone else would like to address the question with regard to Gramm-Leach-Bliley, whether that should be applying to them now or in the future.

Yes?

Mr. HENDRICKS. My understanding is that Gramm-Leach-Bliley does not apply to the processors, and one of the reasons was that they do not keep the information. So when they keep the information, it really becomes problematic.

Mr. GARRETT. Okay. Does anybody else have a comment on that?

Mr. GORGOL. We would agree to have Gramm-Leach-Bliley apply to the processors as well.

Mr. GARRETT. That it should.

Mr. GORGOL. It should.

Mr. GARRETT. Okay.

And, Mr. Hendricks, as long as you are answering the question, in the situation that we have right now and the descriptions that you have here and I guess in your book as well, is there recourse for the consumer in some other avenue other than through the regulatory scheme from civil action or anything else on those matters to recourse?

Mr. HENDRICKS. That is why I like Visa taking action here. The only enforcement action after all these breaches has been Visa in this case. There have been several class action lawsuits filed after various breaches, and those are going to drag on forever, and the companies, the defendants are going to say, "The law does not apply to us," and they are going to point out more holes in the law.

So there is no simple solution for consumers. It is just an enormous burden on them to constantly be monitoring their credit reports and their credit card statements because the smart thieves are going to wait for the 30-, 60-, 90-day period or even over a year before they use the information, particularly if they get Social Security numbers.

Mr. GARRETT. The other people that can be harmed to a degree, not as much as the consumer can be, but that is the issuing companies and the small, I guess they are called the acquiring banks, the small merchant banks are involved here, because they have to pay for the reissuance of the card.

Can some of you discuss that as far as how they are reimbursed? I understand that sometimes it is in the contract, and sometimes I understand that it is difficult for the smaller players, the credit unions as well, that have to get in under the line here to deal with those contracts. Can some of you address that issue, how that is reimbursed and is made or is not made?

Mr. PEIREZ. Thank you, Congressman. I would be happy to address that in so far as the MasterCard system is involved.

First of all, we provide protection against issuers, large and small, both for the cost of monitoring their accounts as well as for the cost of reissuing accounts if that becomes necessary as a result of a data compromise scenario.

There is no distinction between how those rules would apply to a small or large institution. Indeed, our experience is that smaller institutions tend to take us up on that more often. So that is how it works with MasterCard.

Mr. GARRETT. Okay.

Mr. RUWE. In the Visa world, if there is fraud perpetrated on an issuer, whether it is large or small, there is no distinction as well. They have a system of being able to apply for compensation for that through Visa. It is based on actual fraud occurring subsequent to the event.

Mr. GARRETT. My time is up, but thank you.

Chairwoman KELLY. The gentleman's time is up. Please answer the question and then we have to go to another member.

Mr. GARRETT. I do not know if any of the other gentleman from the other—

Mr. GORGOL. It does not really apply to American Express. We are the only issuer and the only acquirer.

Mr. GARRETT. Sure.

Chairwoman KELLY. Thank you very much.

Mr. Davis?

Mr. DAVIS OF ALABAMA. Thank you, Madam Chairwoman.

Let me follow Mr. Garrett's lead and kind of ask you in the time that I have to react to some of the legislative issues that Congress will wrestle with in the next few months based on distinctions from these various bills.

Let me ask you, obviously one of the differences in the bills around the table is the question of preemption, the question of whether or not State law will be set aside in favor of a Federal standard. Let me ask you, do any of you believe that general State tort laws or general State breach of contract laws that are not specific to data security should be preempted? Is there anybody on this panel who believes that a State breach of contract law that is already in place or a State tort law should be preempted by this bill?

Does anyone have an affirmative answer to support that?

Mr. RUWE. Yes, Congressman. I think Visa would support a national level approach.

Mr. DAVIS OF ALABAMA. So you support a national approach which would take a State breach of contract law that is in place right now and say it cannot be applied even if it is not specific to data security.

Mr. RUWE. That is correct.

Mr. DAVIS OF ALABAMA. What about Mr. Peirez, would you support that kind of standard? Just give me a quick yes or no because of the time.

Mr. PEIREZ. Congressman, I will have to follow up with you and look at specifically what you have in mind in terms of the laws in question.

Mr. DAVIS OF ALABAMA. Well, I mean, the specific question was, preexisting State tort law, preexisting State breach of contract law, it is not specific to data security, you have no position.

Mr. Gorgol, do you have a position?

Mr. GORGOL. I am a little bit out of my league. I would have to get—

Mr. DAVIS OF ALABAMA. Okay.

Mr. Minetti?

Mr. MINETTI. Same here.

Mr. DAVIS OF ALABAMA. You are out of your league or you do not have a position?

Mr. MINETTI. Both.

Mr. DAVIS OF ALABAMA. All right.

Mr. Watson?

Mr. WATSON. As I understand what you are saying, it is not just a preemption of regulations but a preemption of remedies, and I guess one needs to go hand in hand with the other.

Mr. DAVIS OF ALABAMA. So your position would be if they go hand in hand with the other, they should be preempted or not.

Mr. WATSON. Yes.

Mr. DAVIS OF ALABAMA. All right.

Mr. Duncan?

Mr. DUNCAN. I am not absolutely clear on the question.

Mr. DAVIS OF ALABAMA. The question is, preexisting State breach of contract law, not a data security law, but a general breach of contract law that a litigant tries to enforce in State court today, should it be preempted by Congress?

Mr. DUNCAN. Again, from a retailer perspective, I am not sure what the cause of action would be.

Mr. DAVIS OF ALABAMA. It would be—

Mr. DUNCAN. But if Congress is attempting to develop a national standard, then retailers would like to see preemption to the extent that data protection is covered.

Mr. DAVIS OF ALABAMA. Mr. Hendricks, I am not quite sure I have heard an answer to my question yet. Would you like to briefly weigh in on it?

Mr. HENDRICKS. Yes. It would be a really bad idea because contracts are between two parties, and I do not think we want the Federal law jumping in between that kind of relationship.

Mr. DAVIS OF ALABAMA. And let me turn to another scenario. One of the issues or the differences is a question of when you disclose a breach, and the bill that Ms. Bean and I have would, if I can use the shorthand, probably create something of a presumption in favor of disclosure. Some of the other bills would frankly probably create a presumption in favor of nondisclosure.

What if you had this scenario, and I will not, for the sake of time, ask you all to react to it, but what if you had this scenario: What if a company believed that its database was compromised but in no specific instance could it identify a specific breach for a particular consumer? Do any of you believe that a company in that instance should not be required to disclose under Federal law if we pass a standard? Anybody want to weigh in on that?

Mr. DUNCAN. I guess I will start by saying I am not sure: if you think there may have been a breach, but you cannot show particular evidence of—

Mr. DAVIS OF ALABAMA. No, no. Let's say that you know there has been a compromise of your system but you cannot identify the instance of a specific consumer that there has been a breach. Should Congress mandate a company that believes its system has been compromised to go ahead and notify the public or should the

company be able to say, "We know we have been compromised but we cannot tell them the specific instance."

Mr. DUNCAN. I think you run the risk in that situation, if you have notification, that unfortunately we run into with some of the Gramm-Leach-Bliley notices. People receive privacy notices by the boatload, and at some point they stop reading them.

Mr. DAVIS OF ALABAMA. And, Mr. Hendricks, I am going to ask one last quick question and you can respond to the one you want to on this one.

I am interested from hearing from Mr. Hendricks on how other professions handle this. I used to be a lawyer, well, still am a lawyer, just do not have to practice now. In my profession, confidentiality is at the bedrock of what we do. Doctors, confidentiality is at the bedrock of what they do; same for hospitals.

What is the standard, Mr. Hendricks, as someone who is an expert on privacy, for a lawyer who believes that his or her files have been compromised? What are the ethical obligations of that lawyer for notifying the client, and what are the ethical obligations of a doctor or the medical world for notifying the patient if their security or their identity or their information, rather the confidentiality has been compromised?

Mr. HENDRICKS. They basically would have to notify very specifically each client and then take whatever remedial actions were necessary depending on what kind of information was breaches. So it would be some heavy lifting, yes.

Mr. DAVIS OF ALABAMA. So that is the current ethical standard.

Chairwoman KELLY. The gentleman's time is up. Thank you very much.

Mr. McHenry?

Mr. MCHENRY. Thank you, Madam Chairwoman. As votes are approaching, I will try to not use up my full amount of time.

I want to start by saying thank you, first of all, to Visa and to MasterCard and to the others for actually disclosing that this occurred. That was not a motivation mandated by law but it was the right thing to do for your customers, and I certainly appreciate you all stepping forward and disclosing to your cardholders and to the public at large that this occurred. I know it was not easy but it was certainly the right thing to do.

And that goes directly to my question for you all, and I will leave this for the panel. Is there a marketplace motivation, is there a market force for data security? We are talking about possibly passing legislation to force you guys to do certain things. My question is, is there a market force for data protection and data security? Now, one at a time. Okay. Slow down here.

Chairwoman KELLY. And please remember that we have been called for a vote, and we need to have answers rapidly.

Mr. PEIREZ. Yes. There is a marketplace for data security.

Mr. MCHENRY. Great answer.

Next?

Mr. WATSON. Congressman, I can tell you there is no stronger marketplace call for data security than the potential undermining of the consumers' confidence in this system. If the consumer does not believe in this system, then we do not have a system and we

do not have a business. What could be a stronger market force than that?

Mr. GORGOL. I would agree. Trust is the bedrock of our business.

Mr. RUWE. We agree.

Mr. PERRY. We agree as well.

Mr. MINETTI. We concur as well.

Mr. MCHENRY. The problem is it is kind of a negative market force that would hit in after the fact, which is why I think we need to get in front of the issue. Inside companies where they have officers who push for security, they still run up against, "Well, why do we really have to do this?" So that is where the public policy has a good role to play.

Mr. Duncan, do you want to chime in?

Mr. DUNCAN. To some extent, it depends on the kind of breach. I spoke with a retailer yesterday who, because they were seeing a fair amount of identity theft, had taken great efforts to reduce that number. Marketplace forces work because they eat those losses.

Mr. MCHENRY. Well, that sounds very encouraging. If there is a marketplace for this to occur, then perhaps legislation is not the right route for us to take. If the marketplace is going to deal with this, let's watch it, let's monitor it, and let's make sure that you all are doing your part to adhere to Gramm-Leach-Bliley, to adhere to the standards we currently have on the books. Let's make sure that is the right thing to do. And I certainly appreciate in particular Visa and MasterCard stepping up to the plate, disclosing fully and doing what was right in a timely manner. That makes a big difference, and it makes a big difference for this committee.

Chairwoman KELLY. Thank you, Mr. McHenry.

We have been called to a vote at the Capitol. I am going to ask the committee to recess for approximately 15 minutes. We will go, we will vote, it is 2 votes, and we will be back here and reconvene in approximately 15 minutes.

[Recess]

Chairwoman KELLY. Let us continue. Thank you for your forbearance.

We turn now to Mr. Price.

Mr. PRICE. Thank you, Madam Chairwoman, and I appreciate you having a recess and allowing us to come back.

You are welcome to take as long as you want answering my questions.

I want to thank you all again for coming, and I want to commend you for the work that you do. I am constantly in awe of the literally billions of transactions that occur without any errors or without any violation at all. And so I want to commend you for the work that you do.

And I understand, as I think Mr. Garrett said, it may have been Mr. Renzi, that there are bad guys out there and they are trying as hard as they can to break your systems, and I think it is important for us to appreciate that we are all on the same team, we are all interested in making certain that the consumer has the confidence in the system and that it works as easily, frankly, as it does now.

Mr. Ruwe, I heard Congressman Renzi say that he had spoken with Visa and with CardSystems and that you all had agreed to

get together and work. I heard Mr. Perry say that, but I did not hear you say that. Are you committed to working with CardSystems and trying to work out a solution that is hopefully more equitable to all involved?

Mr. RUWE. I spoke with Congressman Renzi before the meeting and said I would talk to CSSI. That is what I said. I would meet with them.

Mr. PRICE. And help me understand a little bit about—MasterCard is comfortable apparently right now with allowing CardSystems to continue with the work that they are doing and understanding and I heard a commitment from CardSystems that they would have PCI standards in effect by the end of the month, I believe. How is it that you all reached a different conclusion about your relationship with CardSystems?

Mr. RUWE. I think the crux of our problem is the discrepancies in the audit that we were provided on behalf of CSSI and reality, and there is a huge gap between that, and we feel that CSSI bears responsibility for the accuracy of an audit conducted on their premises.

Mr. PRICE. But CSSI is not the auditor, are they?

Mr. RUWE. They are not the auditor, but they are responsible for what is in the audit report.

Mr. PRICE. Mr. Perry, were you aware—Mr. Gutierrez talked to you about the error being in error and holding that information. Were you aware that you were in error? Was CardSystems aware that they were in error?

Mr. PERRY. Mr. Price, until the incident that took place in May, I was not aware. When I joined the company in April of 2004, I did look at the CISP report prepared by Cable & Wireless. It was an unqualified report, it was a very clean report, and to be quite—I took that report and reviewed it with management, and we were gratified to get the unqualified certification from Visa.

Mr. PRICE. So you thought you were in complete compliance.

Mr. PERRY. Yes, sir.

Mr. PRICE. And to Visa, isn't the culpability here potentially with the auditor and not with CardSystems?

Mr. RUWE. In our system, the culpability is with the party who is being audited. Now, if there is a problem with the audit—

Mr. PRICE. But they believe, however, that they are in compliance because the auditor has told them they are in compliance.

Mr. RUWE. Then I think that if you look at the audit finding versus what turned out to be reality in the environment, the gap is quite large, and we do not understand how there could be a gap of that size between what was true in the environment and what was in the audited report. I do not know what went on between the auditor and CSSI, but it is a joint responsibility in our view.

Mr. PRICE. But you are willing to work with CardSystems and see what that discrepancy was and see if you cannot work out a relationship.

Mr. RUWE. We said we would take a meeting on that. We have asked for explanation on this gap previously and not received satisfactory answers.

Mr. PRICE. Okay.

Mr. Hendricks, I would like you to comment, please, on the sense that I believe is possible and that is a chilling effect in the industry if in fact the individual who stands up and says, "Look, I am in error here, and I am working as hard as I can to comply or correct the situation," what about that chilling effect?

Mr. HENDRICKS. Well, yes, we always want people to have full reporting, so we take the remedial measures and make sure it does not happen again. I do like to focus on the fact that there was a decision made by somebody to keep personally identifiable information that was not allowed by contract. And we have to find out why that happened, why that decision was made, because that is what created the problem, what is exposed here today.

And I think Visa deserves a lot of credit, because if they know that there is a huge gap there and security is not being protected, they have to take enforcement action; otherwise, they become complicit in it and other processors will think, "Well, they do not take this seriously either."

Mr. PRICE. And I appreciate that. And nobody wants there to be these violations or breaches, understanding that no loss occurred as a result of this, is my understanding.

Mr. HENDRICKS. I mean, in terms of loss, I do not think we really know how much the bad guys got and what they did with it. The whole point that they are in the system for over a year and we only have a record of the stuff going out the back door one month, I look forward to the results of the investigation.

Mr. PRICE. Thanks.

My time is up, Madam Chairwoman, but I look forward to being able to submit other questions.

Chairwoman KELLY. And, certainly, you may.

I would like to ask about the PCI standard. The PCI standard, according to page 6 of CardSystems' testimony, is based on Visa's CISP, and it was adopted by Visa, MasterCard, Discover, American Express, Diner's, and JCB in December of 2004.

In theory, the PCI standard did not work here, if you look at it. So are you still using the same standard or has the standard been changed?

And let's start with you, Mr. Peirez.

Mr. PEIREZ. Thank you, Madam Chairwoman.

I think I would say that the standard is relatively new in terms of being an industry standard and only having been implemented at the end of last year, the compliance date for everyone was June 30th of this year.

We, at MasterCard, have gone out with letters to the over 300 third party processors of whom we are aware, making them crystal clear on those standards as well as requiring them to provide us with a certification within 60 days that they are not storing the type of sensitive data that led to this particular breach event. So we think the standards are still sound. We think they were not followed here.

Mr. RUWE. I would like to, if I can, take an opportunity to clarify one thing. The PCI standard became effective in December of 2004, which was the result of the four large card companies getting together and agreeing on a set of rules. However, prior to that, the Visa standards were fully in play and people were fully responsible

to be compliant with them. So in the timeframe that we are discussing here, prior to 2004, the CISP standards would have been in place and Visa players would have been responsible for being compliant with them.

As far as whether or not they work, I think that the CISP standards do work if they are followed. And in this case, up to this point, it appears to us they were not followed.

Chairwoman KELLY. Anyone else like to respond to that?

Mr. Gorgol?

Mr. GORGOL. I agree. I believe the standard is sound. I believe it is an enforcement issue here.

Chairwoman KELLY. Mr. Minetti?

Mr. MINETTI. I also believe the standard is sound. Again, it is just not following the standard that created the problem.

Chairwoman KELLY. Okay.

Mr. DUNCAN. Madam, may I—

Chairwoman KELLY. Yes, by all means.

Mr. DUNCAN. One of the things from the retail perspective, the standards are an excellent idea in terms of trying to work out a coordinated approach, but they are extremely complicated, and that may be part of the issue. Some retailers have mentioned difficulties with the complications as well.

Chairwoman KELLY. Thank you. Thank you for that observation.

That goes to a question I would like to ask of Mr. Gorgol.

In your testimony, on page 2, your explanation of the PCI standard, I would like you to define those standards in light of what Mr. Duncan just said, in terms of their impact on small business customers. Do you impose the same security standards on small businesses for the privilege of using your card that you impose on large businesses?

Mr. GORGOL. Yes, to answer your question directly. I think the standards to protect the data need to be the same for everyone throughout the transaction chain. I think it is incumbent upon us as an industry to make it easy as possible for the small mom and pop stores to be able to meet those standards.

Chairwoman KELLY. Mr. Duncan, you said you think they are a bit complicated. I am concerned because, as I read Mr. Gorgol's testimony outlining some of the expectation levels here, how a mom and pop store, just a small business retail store on a corner, can maintain the six elements of what Mr. Gorgol's testimony—you probably have the testimony in front of you, I can go through them if you do not remember what they are—but I am concerned about its impact and the cost on small businesses.

Mr. DUNCAN. Ideally, there should be risk-reward basis in the standard, and I think there has been some effort to achieve that; that is, that at the original CISP standards there were more requirements for larger merchants than there were for smaller merchants. And this makes a certain amount of sense because if there is a breach, it is likely there is going to be more data captured from a large merchant than a small merchant.

That said, I have heard a number of merchants complain about complications in understanding the enforcement standards, but they are making their best effort to do so.

Chairwoman KELLY. Well, I think we need to make sure that the cards must be secure, that the standards of the industry may not need to be all the same for every industry. It may be a little more difficult for someone in the situation I described, the business person in the situation I described, to, for instance, to keep a written notebook.

Looking at the standard, they were to build and maintain a secure network. Obviously, that is possible. Protect cardholder data. That is possible. Maintain a vulnerability management program. I am not sure what that means. And I do not know how complicated that is. Does that mean you have to have a notebook, you have to have somebody outside coming in to audit? How expensive is this protection?

You have to implement strong access and control measures. That is totally possible for somebody in a small retail business. Regularly monitor and test networks. That is possible. Maintain an information security policy. What does that say?

Those are some problems I see for small businesses, Mr. Duncan. I would like you to answer them.

Mr. DUNCAN. Well, for a number of small businesses, it can be a challenge. You think of a modest retailer that might have 6 or 10 stores in their chain. Chances are they are buying their equipment, the point-of-sale equipment already in a single package, and they really have to rely upon the software and hardware provider to have it right. They probably do not have the facility to do an in-depth study.

So there have to be some allowances for this, and, as I said, it is a challenge.

Chairwoman KELLY. It is a challenge, but I think it is important that we consider this, that the major credit card companies consider this. Having been a retail merchant, a small merchant, and accepting Visa, MasterCard, American Express in my business, I know that I would have been surprised if somebody walked in the door and said, "How are you protecting this information from someone from the credit card companies? Do you take it on faith, do you go and inspect?" What are the standards that you are asking small businesses to do to protect the information at that level?

It is a concern, it is a cost to small businesses, and it is something I think that we need to think about in terms of protection, both for the customer and the retail merchant as well as the credit card issuer.

That being said, I want to go to the concern that I think many small businesses—again, customers of Merrick Bank through the credit card systems will lose their access to credit cards. That could drive them out of business. Was the impact on small business customers considered when the decisions were made from Visa and MasterCard and so on?

What are you doing, Visa, in particular, to help the small businesses stay in their card network?

Mr. RUWE. When Visa selected October 31st as the termination date, as has been stated, we took into consideration how much time it would take for an acquirer to move from one processor to another, and that was felt to be a reasonable amount of time.

I believe the statements that have been made regarding the small merchants' inability to move or inability to retain new services or the situation where they would be out of touch or unable to operate or transmit or conduct Visa transactions have been overstated. We believe that they will be able to find new processor accommodations within that timeframe, and that is something we will work with our banks on, our acquirer banks.

I have not heard this complaint from my acquirer banks. I have only heard it from CSSI. So if my banks tell me we need more time, then we will take that into consideration. We are not going to leave merchants hanging, but the statements that have been made so far regarding merchants and being cut off and being left in the cold have been overstated, in our view.

Chairwoman KELLY. But have you done any outreach on that score to allay the fears of the merchants?

Mr. RUWE. That would be done through the acquiring banks who have the direct relationships with the merchants. That is not done by Visa.

Chairwoman KELLY. All right. I understand that. I mean, I appreciate your response.

When a merchant says to me, "I am not going to accept American Express, I will accept Visa," that is your brand. What has happened here with CardSystems affects your brand. And I understand your wanting to protect your brand, but I also want to make sure that we set standards in such a way that the industry can respond in a way that it is possible for them to. A law is no good unless it can be followed.

So it is extremely important that outreach be made, I believe, from your brand to the small businesses to help them understand not to panic, because from what I understand you are letting the banks take care of that, but, sir, are you sure that the banks are actually in touch with their small businesses and helping them understand and get through and find access to what they need?

Mr. RUWE. Madam Chairwoman, we have every intention of working with the acquiring banks and to support them any way we can in this space. My response was more of a factual one than anything else. We do not have direct contact with merchants any more than we have direct contact with cardholders, but we certainly will support our acquirers in this transition. Whatever we need to do to support them or make sure that the merchants are comfortable and feel knowledgeable about what is going on, we will support them in that regard, yes.

Chairwoman KELLY. I would be interested in Am Ex and Discover's response to that, as well as MasterCard.

Mr. GORGOL. Well, American Express will be offering our merchants a different choice for processing. They will have a number of different options. We will work with them directly over the next couple of months, including the option to come directly to American Express and avoid using a processor all together.

Mr. MINETTI. From our perspective, we have not finalized a decision. We wanted to be thoughtful and have all the information before we reach a conclusion. We have been working with CSSI all along, and we have a meeting scheduled to talk to them next week.

Chairwoman KELLY. Thank you, Mr. Minetti.

Mr. Peirez?

Mr. PEIREZ. Madam Chairwoman, similar to Discover, we have not shut off CSSI at this point. We expect them to be in full compliance by the end of the August, as they have told us they can be. If it becomes necessary for something to happen that would put their ability to process MasterCard transactions at risk, we would certainly make sure that the small merchants would not be impacted in any way. We would do the outreach necessary to get to that point, but we are not there at this time.

Chairwoman KELLY. Thank you.

Yes, Mr. Perry?

Mr. PERRY. Madam Chairwoman, may I just add that I have been in this industry for a long time with quite a few different payment processors, and we have 110,000 small businesses around the United States that are typically not 6-location merchants but one-location merchants, one-location restaurants, and some of those restaurants take up to 80 percent of their sales, or credit card sales, if not 100 percent.

It is my belief that it will not be possible to move a portfolio or part of a portfolio of 110,000 mom and pop merchants over the course of 3 months in an orderly fashion. Changing your credit card processing is not similar to changing your cell phone service, and some of us that have done that also understand how difficult that can be.

There are a variety of different issues involved, including underwriting, technology, changing bank accounts, scheduling, as we all know is very difficult with a small business because at the end of the day they are very focused on moving product out the door, not necessarily the payment type that they take. And this will be a huge inconvenience to the small business, and we are very, very concerned how we continue to take care of these small businesses.

Chairwoman KELLY. Thank you.

Mr. Cleaver, thank you for returning.

Mr. CLEAVER. Thank you, Madam Chairwoman. I have 6,000 questions. I will reduce it to five.

One of the personal issues I have shared, and maybe Mr. Hendricks can respond, about 4 weeks ago the host of one of the "hate" radio shows in my hometown went on the air and said that he had my Social Security number, and he said on the air, "And I plan to use it to find out everything about him." I called the FBI. They said, "Well, we do not get involved in this." I called the Federal Communications Commission and they said, "Well, we do not get involved in this." I ended up calling four or five different Federal agencies, and finally I called the U.S. Marshals Office and they began to monitor the radio show.

It seems to me that there ought to be something wrong with somebody essentially promoting identity theft. And it was done on radio, the record is there, the tape is there, the whole 9 yards, but there is apparently no law against that. I did not think it was a good idea that people could promote the commission of a crime, but apparently you can do it with impunity on the public airwaves.

Is there anything or any way that you think that kind of thing can be corrected?

Mr. HENDRICKS. Well, first of all, I am really sorry to hear that. That is absolutely horrible, and I cannot imagine someone can do that without being ashamed of themselves, but obviously—

Mr. CLEAVER. No, he is not ashamed.

Mr. HENDRICKS. Yes. Obviously, he did. We in the privacy and consumer community would like to see a rollback of the Social Security number. It is required for many things in our society, but we need to start getting them out of courthouses, we need to stop using them as insurance company identification numbers if they are doing insurance. And there is legislation pending to have better protections for Social Security numbers so that he could not get it in the first place. That is the first thing.

Obviously, using a Social Security number to harass someone, yes, maybe that is not covered by statute now but that is something that we should consider looking at.

And in terms of the other problem, where does the consumer go for help, and I have to point out that in every other Western country except the United States there is a national office in charge of privacy issues, where people can go to get answers to these sort of questions, and sometimes you can get an investigation. It is called a privacy commissioner or data protection commissioner, and I think as big as this issue is getting, I think we should start revisiting that issue, because I think we need one here for situations like this.

Mr. CLEAVER. Thank you.

My other question—this will be the last, Madam Chairwoman—I was the mayor in Kansas City and in an attempt to confuse the crooks, we encrypted our system, communications system, so that people who had the radio ban sitting around would not know what we were doing and when we were going to do it. Is encryption an option for us that could possibly either reduce or prevent identity theft, particularly with credit cards?

Mr. DUNCAN. Congressman Gutierrez—excuse me, Cleaver—

Mr. CLEAVER. He is shorter.

[Laughter.]

Mr. DUNCAN. What am I doing? Encryption can be a partial solution, but there are tradeoffs with encryption. There is highly detailed information on credit cards, but obviously we do not want to have stores retain informatin that one could use to make a clone card. But there is fairly basic information, the original numbers, the name, the expiration date, that if you encrypt it, you may save some problems, but you also may create more problems on the other side. Let me give you an example.

Many consumers go into a retail store where they have bought something and they would like to return it but they do not have their receipt. If the checkout clerk who is taking the item back has to decrypt data in order to accomplish a return, it makes it much more difficult or maybe impossible in many situations. So there has to be a balancing as to how we achieve that.

As to your first question, may I say that one of the points we wanted to focus on in our testimony is the need for more enforcement. Currently, if retailers find evidence of identity theft and take that to the State attorneys general offices, oftentimes they will not enforce unless they have $100,000 worth of damage. So we would

like to see a situation where Congress would encourage State officials to take a more active role in going after those who are committing crimes.

Mr. CLEAVER. Thank you.

Chairwoman KELLY. Thank you, Mr. Cleaver.

Mr. Price, you said you had another question. Feel free to ask.

Mr. PRICE. I may?

Chairwoman KELLY. Yes.

Mr. PRICE. Thank you, Madam Chairwoman. I appreciate it.

I think this is an incredibly important topic, and I think we can overreach in so many ways, but, again, I think it is imperative that we make certain that folks have confidence in the system.

Mr. Gorgol, if you would not mind, please, commenting on the potential culpability of the auditor vis-a-vis CSSI review and ultimate problems that they had.

Mr. GORGOL. We relied via our contract on CardSystems meeting their contractual obligations to meet the data standard. And they were the ones we worked with. We did not work directly with the auditor, so I cannot comment on it.

Mr. PRICE. Mr. Duncan, there has been a discrepancy between responses on the effect on merchants with the cessation of the relationship between Visa and CardSystems. Would you comment on what you believe that consequence would be or the effect on merchants?

Mr. DUNCAN. We are not privy to all the details involved in this dispute. Obviously, as in this whole issue, you do not want to overreact in a credit card fraud situation as opposed to, say, an identity theft situation. And this strikes me as one where the risks are perhaps lower than a true identity theft, and so maybe that same guidance should apply.

Mr. PRICE. Mr. Ruwe, I have affinity for Mr. Perry and CardSystems, obviously. I also think, again, we are all on the same team in this in trying to make certain that violations of information do not occur. Do you believe that Visa's relationship with CardSystems is fatally flawed?

Mr. RUWE. Well, fatal is a very big word.

Mr. PRICE. Yes. That is what is going to happen to them.

Mr. RUWE. It is certainly stressed. I think that Visa spent a great deal of time trying to evaluate what position we were going to take on this, and I believe we made several attempts to get information that we needed and did not get it. And as we said earlier, we will sit down with CSSI, but I think we are going to have to have more information and more forthcomingness, if you will, than we have had to date before I would make any commitment on anything fatal or otherwise.

Mr. PRICE. I appreciate that. If I am able to facilitate any of that, please let us help.

Mr. Perry, I would like you to comment, if you would, on the discrepancy that Mr. Ruwe pointed out or stated existed between the audit and the reality of the information that you all held.

Mr. PERRY. Yes, Mr. Price. We did receive some requests from Visa for information regarding the discrepancy between the CISP audit and what was subsequently found by the forensic analyst. Unfortunately, I was able to provide to Mr. Ruwe and Visa all of

the data that I was able to find prior to my arrival at CardSystems in April of 2004. We stated to Mr. Ruwe and some of his associates at Visa that we were providing all of the information possible.

We attempted to contact former employees, former auditors from Cable & Wireless and other former vendors to be able to fully answer Mr. Ruwe's questions. Unfortunately, it was very difficult to track a lot of these people down who had left the company sometime in 2003, early 2004. And, unfortunately, because we were not able to provide all of that information, it was deemed that it was not enough information.

Mr. PRICE. Help me with the audit. Was there an actual question on the audit that said, "Is CardSystems in full compliance with the agreement with Visa?" Is that the kind of question that is on there?

Mr. PERRY. There are several questions that you would see in an audit that are fairly detailed as to very different aspects of the audit having to do with network security and, specifically, the error that we have owned up to, which is the storing of this data that should have been masked. And that is a specific block or question. That specific block had a checkmark by the auditor without qualification or any compensating controls in that area.

When I specifically reviewed—

Mr. PRICE. Checkmark saying?

Mr. PERRY. We were compliant. When I reviewed that, I felt pretty good and relied upon the audit and the auditor that we were in compliance in that area.

Mr. PRICE. May I ask one more general question, Madam Chairwoman?

I am interested from all the card companies as to whether or not there is agreement or consensus in the industry about the definition of a data breach and fraud. Is there consensus among the companies about what that is?

Mr. PEIREZ. Congressman, I think there is general consensus on what would constitute credit card fraud. In terms of your question about breach, it is a very complicated question, and I think we are in general agreement, but any specific case you would have to look at the specifics and see whether we all agree.

Mr. PRICE. Mr. Ruwe?

Mr. RUWE. I would concur with that.

Mr. MINETTI. Yes, I would agree as well.

Mr. PRICE. Is there a need to define those terms? Are they defined legally as it relates to data breach?

Mr. PEIREZ. Congressman, I think that, first of all, the terms that most often get confused and really do need to be used carefully and accurately are the distinction between fraud and identity theft or identity fraud. Those are the two things that really need to be very, very clearly identified because the consequences of either of those events are quite different and can be handled in different ways effectively.

In terms of definition of breach, I think that depends on what happens if there is a breach as so defined. So I would be happy to work with your office if you are looking at something specific, but as to the general question on breach, I really cannot answer.

Mr. PRICE. Any other general comments about that?

Mr. WATSON. I would say that the language is unclear, and it is unclear with respect to impact and timing. For instance, you could say the system was breached in April of 2004. Accounts were compromised possibly at some other time and certainly in May of 2005. But the definitions are not clear with respect to time or effect, and I think in putting forth any legislation they are going to need to be very clearly defined.

Mr. DUNCAN. Congressman, there is one additional element, and this goes back to the question that the chairwoman mentioned, and that is for smaller retailers in particular, if they are buying off-the-shelf equipment, they want to make certain that if they bought something from IBM or NCR or something else, that they are not deemed to be in breach because of something they innocently purchased. And that is a distinction that has to be maintained.

Mr. HENDRICKS. The California State law does a pretty good job of defining a breach by saying it is personal information or account numbers/Social Security numbers that can be used to commit fraud. And as to the distinction, there is a distinction between identity theft takeover and credit card fraud, but under the Identity Theft Deterrence Act and under FACTA, Congress has defined some forms of credit card fraud as identity theft, as it should, because we need to maximize protection for consumers, and you see this reflected in FTC regulations.

So I agree with industry that we need to look very carefully and draw these distinctions so we have appropriations responses to each one, but I want industry to respond that some forms of credit card fraud are also identity theft.

Chairwoman KELLY. Thank you.

Mr. PRICE. Thank you, Madam Chairwoman.

Chairwoman KELLY. Thank you, Mr. Price.

Mr. Cleaver, you said you had another question or two.

Mr. CLEAVER. Admittedly, this is personal for me, but I am curious as to whether other Western countries, Mr. Hendricks, have strong laws with regard to identity theft. When I say strong laws, I mean when there is a data breach it could result in someone being just wiped out.

So do you know of any other country where someone could do something and actually regret it?

Mr. HENDRICKS. Do something in terms of using personal information?

Mr. CLEAVER. Yes.

Mr. HENDRICKS. Well, a lot of the European countries and others do not have the biggest problem with identity theft as we do because they do not rely on the Social Security number the same way that we do. So they do not have specific laws on identity theft.

Mr. CLEAVER. What do they rely on?

Mr. HENDRICKS. Well, they have their own usually national identification number or another set of identifiers. We need a country-by-country report. It is a very long question and answer. But they had old-fashioned comprehensive laws which are based on what we know as fair information principles, and that ends up covering a lot of these sorts of events.

So they are constantly trying to upgrade them and oversee and implement them, but it becomes more of a compliance issue be-

cause they have a general framework which covers most personal information, creates rights for individuals, duties on organizations.

Mr. CLEAVER. I do not know if you collect data that would provide information about how long it would take after a breach before the fraudulent act begins. And is there any data that would allow us information to know the time between the breach and the time of the commission of a fraud?

Mr. HENDRICKS. There is no real research on that has been made public, but it ranges from immediate to long term. The methamphetamine users that hit mailboxes they try and use something right away, that is just their nature. The very sophisticated criminal rings will sit on information and use it down the road.

Mr. CLEAVER. So my radio host is sitting on it.

Mr. HENDRICKS. Yes, but I think maybe someone should sit on him. I think he deserves some more attention.

Mr. CLEAVER. Thank you.

Chairwoman KELLY. Thanks, Mr. Cleaver.

Mr. Gorgol, you raised a very important issue in your testimony and we have not talked about it, and that concerns phishers with a "ph." I think you mentioned that you were concerned that phishers might take advantage of the breach and other publicized incidents to look around to see what they can find from card customers.

I would like this panel to describe whether or not you have seen a reaction like that in this case, and I would also like to know whether small businesses are likely to be contacted by fraudsters that are claiming to represent interested parties in this case?

And with the terminations and so on that are imminent, apparently, I am wanting to know what you are doing to reach out to small businesses to keep them secure from phishers who are likely to call them and say, "We are checking on this information," and so forth. They do not know who is at the other end of the phone. I want to know what you are doing to protect these people from a fraudulent inquiry and a fraudulent solicitation during the changeover period.

Mr. GORGOL. Well, first, I mean, phishing is a serious problem and I think it is something to consider if we think about legislation that requires notification. If we overnotify people, that will provide, I think, a vehicle for phishers, sort of weeds that they could hide in if we overnotify. It is one of the dangers of overnotification.

But I think the most powerful tool we have, to answer your question directly of what we can do and how we can help small businesses, is education and just raise their awareness that phishers are out there and just be very careful in how they share their information.

Chairwoman KELLY. How do they know if someone calls and says, "I represent such and such, and I want this information"?

Mr. GORGOL. There are basic rules. They are not to share personal identifiable information over the phone unsolicited or you are not sure who you are sharing it with.

Chairwoman KELLY. Well, if they are solicited, they are going to share it because they do not know the difference. My concern is that there be some sort of an interception there, direction, edu-

cation, however you do it, so that the small businesses during the changeover will not become a victim of phishing.

Mr. GORGOL. Well, during this specific changeover, they would be working directly with American Express employees, so we will be able to contact them directly.

Chairwoman KELLY. Anybody else?

Mr. Ruwe?

Mr. RUWE. I think that would add to the education, and part of the education is making sure they understand that if they get one of these calls, that they should say, "Thank you very much." And they have been trained to say, "Give me a number where I can call you back, please," and then they can verify with their true business relationship. That is one of the things that we have tried to reemphasize over and over again in our educational materials.

But, typically, the phishers do not necessarily target small businesses. They may be affected by this, but they really go for the big broadcast over the Internet. That is why it is called phishing. They go out and really attack the masses is usually their MO.

Chairwoman KELLY. In the 1970's and 1980's, a number of banks spun off the card processing units and now some of the banks are bringing them back in-house. There are pros and cons on this, and we have not heard from any of you about that.

Mr. Watson, you may be the first one to answer that question. What are the pros and cons?

Mr. WATSON. I actually have worked for data processors in the past prior to my career at Merrick Bank. I think data processing for both card holder and merchant business is very, very much a scale issue, and in-house processing is really only affordable by the very, very largest issuers and the very, very largest merchant banks.

Without the access to high quality, secure third party processors, the credit card business, both the issuing side and the merchant banking side, would be in the hands of a very, very small number of banks because they would be the only ones who could afford it.

Chairwoman KELLY. Okay. So you think that unless a large bank like Bank of America, Citi, Chase made the decision to bring it back in-house, no one else is likely to because it is expensive; is that correct?

Mr. WATSON. Yes.

Chairwoman KELLY. Okay. Thank you.

My last and final question to you, Mr. Perry, there was a 3-day time lag between the time you discovered that there was a problem in the system and the notification that went out, you called the FBI, but it was not until the next day, it was basically a 3-day time lag. You found out on the 22nd and on the 25th Merrick Bank found out and the card people found out. What caused that time lag?

Mr. PERRY. Madam Chairwoman, the time lag was we found out of a suspicious production issue on Sunday, late afternoon, Sunday, May the 22nd. On Monday, May the 23rd, we contacted the Phoenix office of the FBI and on actually Tuesday, May the 24th, we had not heard back from the Phoenix FBI and then contacted the Atlanta FBI because we were very concerned that this might be a situation that law enforcement needed to be aware of immediately.

Once we heard back from the FBI on the 25th that they had assigned a case officer and we had disclosed everything to them, we also asked if it was okay under the investigation to contact the bank and notify the bank so they could go through their proper notification procedures, and they said, yes. Unfortunately, there were 2 days of lag where we missed speaking to the FBI from Atlanta or Phoenix to receive proper instructions.

Chairwoman KELLY. So the time lag, if I understand you correctly, was caused by the FBI not getting back to you in a timely manner. In the meantime, the 44 million people whose information had been perhaps compromised were still out there with their information compromised and nobody knew it.

Mr. PERRY. At that time, all that we were aware of was the export of the 239,000 discrete cards that we found about later. I do not want to say that the FBI did not react, but we did contact the Phoenix office on Monday, and when we did not hear back from them on Tuesday we contacted the Atlanta office. At that point, both offices coordinated and once they got back to us, we also asked them if we could move to the next step of notification, which we saw as critical, which is contacting our sponsor bank, Merrick Bank.

Chairwoman KELLY. I am just curious because under a contractual agreement with the credit card companies, wouldn't that have been in the contract that you had to notify them immediately if you discovered any kind of a breach?

Mr. PERRY. At that point, on May the 22nd and even on May the 23rd, we were unclear as to the scope of the potential compromise.

Chairwoman KELLY. But you knew you would been compromised.

Mr. PERRY. We believed we had, yes.

Chairwoman KELLY. But it was just a matter of degree. So if there was a contractual agreement for notification to the credit card people—

Mr. PERRY. Because we believed there had been a crime perpetrated against the company and its merchants, we believed it was incumbent upon us to contact law enforcement first and make sure that they would help us and guide us through this situation. This is a situation that we had not previously experienced in the past, and we wanted to make sure that in no way would we compromise any future investigation.

Chairwoman KELLY. Thank you.

I want to thank this panel for your patience. You have been wonderful for staying with us, and I appreciate very much the fact that you have given us so much of your time and your expertise today.

The Chair notes that some members may have additional questions for this panel, which they may wish to submit in writing. So without objection, this hearing record will remain open for 30 days for members to submit written questions to the witnesses and place their responses in the record.

This hearing is adjourned.

[Whereupon, at 1:12 p.m., the subcommittee was adjourned.]

A P P E N D I X

July 21, 2005

Statement of Congressman Michael N. Castle

Oversight and Investigations Subcommittee Hearing on
"Credit Card Data Processing: How Secure Is It"

July 21, 2005

Thank you Chairwoman Kelly and Ranking Member Gutierrez for holding this important hearing today before the Oversight and Investigations Subcommittee. As a member of the full committee but not of this particular subcommittee, I would also like to thank you for the opportunity to attend.

In recent months, a number of "data breaches" have come to light. We know of at least 50 breaches of database security that have occurred since the beginning of 2005 that, taken together, could impact over 51 million Americans. Among the most troublesome is the CardSystem breach we are examining today. The initial reports of 40 million consumer accounts compromised has heightened consumer awareness of this issue. While I am thankful this initial number appears to be well above the number of cards actually exposed, which I understand is closer to 200,000, this is still 200,000 too many. I've read that CardSystems was not following the "Payment Card Industry Data Security Standards" as required by Visa and MasterCard -- if this is true, this is a lapse that should not have occurred.

I strongly believe that something must be done on a federal level to ensure sensitive data is being properly protected. To this end, I am pleased to have introduced legislation today with the Gentlewoman from Ohio, Ms. Pryce, and the Gentleman from Kansas, Dennis Moore, which would address this by creating uniform national security standards for sensitive data as well as consumer notification and mitigation procedures in the unfortunate instance in which a breach occurs.

While our financial institutions, as defined by the Gramm-Leach-Bliley Act, are already required to secure their sensitive data, we must ensure this standard is being enforced and clearly in light of problems in the retail and data broker sector need to ensure it is extended it to all sectors that have sensitive consumer information.

As we examine this and other data breaches, I believe we must understand the facts of each case and use information as we work to create a national standard. Does losing an account number pose the same risk as a breach that includes a consumer's name, address and social security number? When consumers are notified are they taking the proper steps to protect themselves from future harm? And frankly, are they even opening the envelope from the breached entity to inform them that their information has been placed at risk? These are all questions that we must answer as we move forward on legislation and I look forward to hearing from our witnesses today.

The flow of information in our society is important -- it helps consumers everyday with access to credit, price competition, and even with issues related to public safety -- but we must ensure that sensitive information has a standard of protection around it that extends to all sectors handling the data. Simply put we can not have a gap in the system. Madam Chairwoman, I thank you for holding this hearing today and again, I look forward to hearing from each of our witnesses.

COMMITTEE ON TRANSPORTATION
AND INFRASTRUCTURE
CHAIRMAN, SUBCOMMITTEE ON RAILROADS

COMMITTEE ON
FINANCIAL SERVICES

COMMITTEE ON
GOVERNMENT REFORM

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

Opening statement of Congressman Steven C. LaTourette
July 21, 2005
Subcommittee on Oversight and Investigations

Chairwoman Kelly, thank you for holding this hearing today on what has become a critical issue for this Committee.

When I flip back through the last few months of financial services news clips, I have to ask myself, how have we allowed our data security standards to get so lax as to allow tens of millions of American consumers' sensitive information to be put at risk? If we look across the pond, we as a nation are a good decade behind Europe in terms of stringent rules guarding the protection of consumer data.

This morning, my colleague Darlene Hooley and I introduced legislation creating a national standard requiring financial institutions and the many "data brokers" that compile sensitive, financial information about American consumers to send a uniform notice to consumers whose information was put at risk due to a breach or compromise of data. Our bill, the Consumer Notification and Financial Data Protection Act, puts the burden to safeguard data where it belongs – on the numerous entities that maintain our financial data – and requires them to take the necessary steps to investigate and remedy a security breach if one occurs. It also makes sure affected consumers know what's going on, how they can protect themselves further, and makes available to them a year of a free credit file monitoring service.

In addition to the introduction of our bill, my colleagues on this Committee Deborah Pryce, Mike Castle, and Dennis Moore also introduced legislation on this issue today. The Financial Services Committee has a long record of protecting consumers and their credit from financial fraudsters. With these two bills, this Committee can now continue the process of making sure that the bill considered by the full House is the best solution for American consumers and industry.

This is our opportunity as a Committee to continue the good work we did by passing the FACT Act. This hearing today, in retrospect, is a direct result of that legislation, because without it, our nationwide credit system wouldn't exist. There's no doubt in my mind that our system has been an invaluable asset to countless people, but obviously it is not without its faults. Finding a solution to protecting American consumers when companies suffer a breach of data security is a critical first step, but it is not the end of what I believe we should do. There are larger data security issues that need to be addressed, and I look forward to opening a dialogue with our panelists today.

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

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

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

P.O. BOX 1132
TWINSBURG, OH 44087
(330) 425-9291

STATEMENT OF THE

NATIONAL RETAIL FEDERATION

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

COMMITTEE ON FINANCIAL SERVICES

"CREDIT CARD DATA PROCESSING: HOW SECURE IS IT?'

THURSDAY, JULY 21, 2005

Good morning I am Mallory Duncan, Senior Vice President and General Counsel for the National Retail Federation. I appreciate the opportunity to testify at today's hearing. By way of background, the National Retail Federation is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet and independent stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.4 million U.S. retail establishments, more than 23 million employees - about one in five American workers - and 2004 sales of $4.1 trillion. As the industry umbrella group, NRF also represents more than 100 state, national and international retail associations.

The Nature of the Problem

There has been a substantial increase in reported incidents of identity theft over the past several years. Precise year-to-year comparisons among the competing estimates are difficult to make because the methods of measuring prevalence, awareness of the issue and the definition of the problem itself differ significantly among those who are reporting and those keeping track. In May, 2003 the Department of Justice, in conjunction with the Solicitor General of Canada, issued a Public Advisory and Special Report to retailers on identity theft. At that time, the Department of Justice indicated that identity theft complaints to the Federal Trade Commission ("FTC") had increased fivefold since 2000, from

31,117 to 161, 819 in 2002. The Canadian PhoneBusters National Call Centre received 7,629 identity theft complaints in 2002 with reported total losses of $8.5 million. The advisory further indicated that two major Canadian credit bureaus received approximately 1,400 to 1,800 complaints of identity theft per month. On February 1, 2005, the FTC released its 2004 complaint numbers. Again, reports of identity theft continued to climb, reaching 215,093 in 2003 and 246,570 in 2004[1]. Recently, the FTC completed a national survey in which it projected approximately ten million people experienced identity theft within the past year. Even larger numbers have been published elsewhere.

As striking as these figures are, it is important to recognize that the frauds they reflect comprise a variety of activities, not all of which are true identity theft and not all of which are susceptible to the same analysis or solutions. For purposes of today's hearing, let me explain what we mean when we speak about true identity theft.

Compared to fifty years ago, we live in a mobile, fragmented society. Relatively few of us reside in the community in which we were born, and even fewer of us have neighbors or shopkeepers who've known us since birth. Although passports and other such documents have long existed, day-to-day proof of our identity has shifted from being something that was known or vouched for by others to something that is inferred from documentation and our knowledge of relatively obscure facts. In today's world, individual identifiers such

[1] The FTC further breaks down identity theft complaints to include: credit card fraud (28 percent), phone or utilities fraud (19 percent), bank fraud (18 percent), loan fraud (5 percent), other identity theft (22 percent), government documents or benefits fraud (8 percent), employee-related fraud (13 percent) and attempted identity theft (8 percent).

drivers licenses or social security numbers, and quick recall of personally-related facts such as date of birth, mother's maiden name, and office telephone numbers, substitute for actual proof of identity. This is an accommodation we've made in order to allow millions of us to routinely travel thousands of miles from our birthplaces to work, to relocate and to recreate. This system worked reasonably well so long as the identifiers were unique, the personally-related facts were largely buried, and the pace of business was slow.

True identity theft occurs when someone appropriates another individual's identifying data for the purpose of secretly assuming that person's identity. For example, a thief, by the name of Susan Kelly may decide to become "Sue Kelly." The thief may associate the real Sue Kelly's name, social security number, date of birth and other facts with her, Susan Kelly's "new" address. The thief may go on to obtain a driver's license, open credit and checking accounts, purchase a car, even buy a condominium, using Sue Kelly's excellent credit history. So long as the thief keeps up her payments or doesn't otherwise draw attention to herself, it might be months or years before anyone discovers the fraud, if ever.

These true identity thefts are the frauds that make the crime of that name so frightening. At some point the thief may decide to start writing bad checks and to stop making payments on the car, the house or the cards, stiffing the creditors and potentially ruining the victim's consumer report. It could take months or years for the victim to recover her or his good name. Worse, if the thief is not apprehended, there is always the possibility that she or he will lay low, wait one,

two or seven years, and attempt to repeat the process again. The victim may need to be ever vigilant.

In contrast, much of what is commonly referred to as identity theft is, in fact, relatively straightforward credit card fraud. While retailers do not by any means make light of it, and it can be a problem for those affected, it is much closer to a serious nuisance than it is to the horror of true identity theft. Equally important, Congress has already provided many of the tools victims need for its correction.

In a typical credit card fraud someone obtains all or enough information from an individual's credit or debit card in order to accomplish a transaction. The crime could be as simple as an attendant making two impressions of a credit card on an embossing machine, and submitting both for payment; or it could be as sophisticated as capturing all of the critical data from a card and creating a phony "cloned copy" of the card that is sold on the black market or used for an intensive shopping spree. Regardless, the individual who's card information was taken will be made aware of the fraud either through a contact from the credit card company, inquiring as to the suspicious activity, or when the monthly statement arrives detailing the fraudulent charges. Congress has provided (under Truth-in-Lending, Fair Credit Billing Act) that the consumer may challenge those charges and, unless the consumer were contributorially negligent, the consumer is held harmless for the loss. Either the retailer or the card issuer bears the burden. I would like to repeat that point: retailers typically bear the financial burden of credit card fraud.

With these distinctions in mind, it is clear that the incidence of identity theft is considerably different than some of the numbers that are cited. While reported cases have been in the hundreds of thousands, even if one accepts the ten million cases estimated by the FTC, on closer analysis it turns out that two-thirds of those are not truly identity theft.

What also is important to note about these two types of fraud is that the remedies are quite different. Credit card fraud is usually a one-off event. Once the crime has been discovered it is relatively simple to stop the thief from continuing to victimize that individual by closing the account and reopening a new account with a different number. Within a matter of hours or minutes the thief's card information essentially becomes useless. On the other hand, when true identity theft occurs, it is not a simple matter to change an individual's social security number, date of birth or mother's maiden name. The tools to commit the crime again remain in the thief's possession. It is for these reasons that it is important Congress not lump these very different frauds into the same basket. If society has limited resources that it can devote to fighting crime, then we ought to tilt toward using those resources to help those confronted with the most serious consequences, e.g. true identity theft.

Thus, fraud alerts and regular monitoring of consumer reports might makes greater sense when there has been true identity theft. They put up a red flag to those who would grant credit, informing them that a thief has been impersonating the consumer and can provide the consumer with an opportunity

to ensure that new accounts are not being opened in his or her name. On the other hand, consumer report monitoring, for example, is virtually useless at detecting credit card fraud. The thief is not opening new accounts, he is running up charges on existing accounts; charges that the consumer can eliminate at month's end. Therefore, it makes little sense to expend huge amounts of money to provide regular monitoring to those who have experienced unauthorized use of their credit cards when those funds might better be spent on other protections, such as even more sophisticated neural networks or improved payment systems.

This underscores another important point. In contrast to the identity theft-sensitive information discussed above, most of the information retailers maintain is fairly innocuous. They may maintain some credit card data. In general, when a purchase is made on a card, the retailer transmits all of the necessary card data to its acquiring bank or processor for authorization. Once authorization is received retailers are directed to eliminate all but the most basic credit card information from their files. Basic credit card information (name, account number and expiration date, but absent the information necessary to create a cloned card) may be retained in order to facilitate customer returns. Beyond basic card data, and independent of the financial services systems, information about prior purchases or customer preferences (e.g. sizes, colors or styles) may be maintained in order to provide more personalized service. Mailing addresses may be used to speed future transactions and for quality or security purposes.

From an identity theft perspective all information is not equal, and none of the foregoing is directly implicated. We have an exceedingly complex economy.

The use of different types of information poses greatly differing levels of risk and provides differing levels of benefit to consumers. If identity theft prevention is the goal, Congress should be especially sensitive to the associated costs and benefits of the type of information at issue, and its usage in various environments, so as to avoid painting with too broad a brush.

What Has Been Done

The growing reports of identity theft led to a significant amount of testimony before the House Financial Services Committee in 2002 and 2003, as part of a series of hearings held on the reauthorization of the Fair Credit Reporting Act. Indeed, this Committee went on to establish many new protections for identity theft victims in the Fair and Accurate Transactions Act (FACTA), including the right to block fraudulent information on their credit reports and the creation of new fraud alert systems so that new credit would not so readily be extended to identity thieves. After extensive rulemaking, many of these new rules and protections are now just coming on-line, and there is still much work left to do.

As members of the Committee are aware, shortly before the FACT Act was signed into law, a new California statute was enacted requiring the public disclosure of security breaches under certain circumstances. This law, and the data security events that it has caused to be made public, has brought the issues of data security, consumer privacy and identity theft to the public's attention like

never before. These highly publicized stories appear to have eclipsed somewhat the important work Congress did to protect consumers just a year and a half ago. The reported breaches have ranged from the mistaken sale of thousands of files full of sensitive personal information to criminals posing as legitimate businesses, as in the case of ChoicePoint, to encrypted data tapes containing account information literally disappearing in the cargo hold of a plane, as in the case of Bank of America. In the retail sector, reported cases have involved criminals attacking and hacking into computer systems in order to steal customer credit card information.

What is telling about the recent media stories is that almost all the large disclosures have involved credit card data, not identity theft data. In some ways this suggests it currently may be easier for thieves to obtain the less damaging type of information. Nevertheless, a great deal of attention has been focused on means of reducing the incidence of credit card fraud. Over the course of this summer, substantial numbers of merchants are expected to come on line with Visa and MasterCard's new card security program. Begun several years ago to protect credit card purchases on the then nascent Internet, the card association are extending the security requirement to cover virtually all credit card transactions.

The FTC recently entered into a proposed settlement with B.J.'s Wholesale Club as the result of one these system attacks in late 2003 that resulted in millions in fraudulent charges on their customers' credit accounts.

Part of the settlement alleges that B.J.s was in violation of the type of bank security rules that I described above. The B.J.'s case, however, has been something of an anomaly, and other reported retail computer attacks, to our knowledge, have been discovered and managed before they have resulted in significant losses.

Retail Specific Difficulties

From a retailer perspective, there are some areas where the damage caused by true identity theft and that caused by credit card fraud can overlap. If a true identity thief is able to apply for and obtain a credit card, he may use it to make purchases, either remotely or in person. Depending on the circumstances the retailer innocently accepting the card may be forced to absorb the cost of the fraud. On the other hand, when full file credit card data is stolen from an entity and enough information is captured to clone that card (create an exact duplicate with an active magnetic strip), it is often difficult for a merchant, or any other entity, to detect that a card used at point of sale is indeed a fraudulent card. Once the magnetic strip is duplicated it allows the cloned card to run over electronic authorizations channels just like an authentic card, and unless the original card has been reported lost or stolen, or the card companies' neural networks have detected potentially fraudulent spending patterns, it will be approved just like an authentic transaction. Nevertheless, the merchant may or may not be responsible for the transaction depending on a variety of factors. As mentioned above, it is the card companies, who are in the best position to

develop these fraud detection systems. They "see" a broader range of transactions, have a larger body of customer shopping pattern experience, and thus are more likely first to discover that a card number breach or cloning pattern has occurred.

This is important because by and large retailers are not in a position to bargain as to the terms of card acceptance. Penalties, requirements and ever-changing rules are largely dictated as a condition of acceptance. While the card systems are premised on mutual benefit, most of the leverage is on one side. We ask that you carefully consider any legislative changes so as not to further disadvantage those who already pay so large a portion of the cost of fraud. To the extent Congress directs its attention to the core problem, true identity theft, this is less likely to occur.

In summary, identity theft is fairly focused, but harmful, form of fraud. Proof of identity has become a more elusive quality at the same time that our society has invested greater amounts of trust in its veracity. Viewed objectively and from a distance our credit granting system seems miraculously facile. Families receive high-quality meals in exchange for a swipe of plastic. Vacationers are able to take possession of cars hundreds of miles from home merely by presenting out-of-state documents and cards. Individuals are able to secure funds to purchase their homes from bankers they have never before met. These benefits flow not from the credit cards, but rather from the trust our society invests in the identities of the persons seeking credit. If we are to preserve

these benefits, society should crackdown on those who would abuse that trust by appropriating the core incidents of identity. With the passage of the FACT Act Congress has begun to provide tools to those who have been victimized; it now should provide funding to ferret out and prosecute those who make the use of such tools necessary.

Thank you for the opportunity to appear here today. I would be happy to answer your questions.

House Financial Services Committee
Subcommittee on Oversight and Investigations
Hearing: "Credit Card Processing: How Secure Is It?"
July 21, 2005

Written Statement of
Zyg Gorgol, Senior Vice President, Fraud Risk Management
American Express Company

Chairwoman Kelly, Ranking Member Gutierrez, members of the Subcommittee, my name is Zyg Gorgol and I am Senior Vice President of Fraud Risk Management at American Express. American Express Company was founded in 1850 and is today a diversified worldwide travel, network and financial services provider. We are leaders in charge and credit cards, Travelers Cheques, travel, network services and international banking.

I appreciate the opportunity to testify today about the recent data security breach at CardSystems Solutions, Inc. and its impact on American Express Cardmembers. We view this breach with great concern and have taken steps to protect any Cardmembers who may have been affected by it. I also want to comment today about American Express' data security standards for merchants and third-party processors. We believe our work in this area is a critical element in helping to ensure that sensitive Cardmember information that is processed on the American Express network remains secure.

Background

American Express operates what is often referred to as a "closed-loop" network. American Express issues charge and credit cards to customers, and also has direct arrangements with merchants who accept American Express Cards. This can be distinguished from an open network arrangement, where the entity that maintains arrangements with merchants for card acceptance is typically not also the card issuer. In an open network environment, the network provider or association serves as a conduit between the issuer and the acquirer.

In terms of data security, which is the focus of this hearing, there is nothing technically more secure in an open or closed loop network. However, we at American

Express have through the years used what we learned from our closed loop environment to build state-of the-art systems to detect and prevent fraud. I believe our fraud prevention efforts have benefited significantly from the valuable information our closed loop network provides.

American Express also operates a Global Network Services business where we partner with select banks to issue cards on the American Express network. In this case, our partners issue cards on the American Express network, while we continue to maintain the merchant relationship. In the United States, MBNA, Citibank, Juniper Bank, and USAA have signed up to issue American Express Cards to their customers.

Payment Card Industry Data Security Standards

The Payment Card Industry Data Security Standards (referred to as the PCI Standards) provide an industry-wide approach to safeguarding charge and credit card customer data. The PCI Standards were developed by a cross-industry working group that included American Express, Visa U.S.A., MasterCard International, Diner's Club, JCB, and Discover.

Specifically, the PCI Standards apply to any merchant or processor that handles any cardholder data. The Standards require merchants and processors to (1) build and maintain a secure network; (2) protect cardholder data; (3) maintain a vulnerability management program; (4) implement strong access and control measures; (5) regularly monitor and test networks; and (6) maintain an information security policy. With respect to protecting cardholder data, the PCI Standards specify encryption standards to protect stored data and transmission of cardholder data and sensitive information across public networks. In addition, the Standards specify that merchants and processors must not

store the full contents of any information from the magnetic stripe on the back of the card or the validation identification code that appears on the card.

While American Express fully endorses these Standards as an appropriate industry baseline standard for data security in the payments industry, we recognize that the PCI Standards do not resolve all issues. Indeed, in the case of the data security breach at CardSystems, the PCI Standards apparently were not followed in a number of important ways.

CardSystems Breach

CardSystems Solutions processes less than one percent of American Express Card transactions. Upon learning of the breach at CardSystems, we began an extensive investigation to determine any impacts on American Express Cardmembers. We also followed our practice of flagging potentially affected accounts and putting additional security and fraud prevention measures in place for those accounts. We are continuing to closely monitor those accounts for any suspicious activity on an ongoing basis.

Based upon our investigation into the CardSystems breach, in which we worked directly with the computer forensics firm Cybertrust, we have determined the following:

- The CardSystems database that was accessed by unauthorized persons contained records of approximately 40 million charge and credit card accounts -- only a small percentage, approximately four percent, of these were American Express Card accounts.
- Our analysis indicates that information relating to approximately 12,000 American Express Card accounts in the CardSystems database appears to have been accessed by unauthorized persons.

- Although the information relating to these 12,000 accounts included the card account number and expiration date, it did not include any personally identifiable information of American Express Cardmembers, such as name, address, or telephone numbers, nor did it include any other sensitive personal information, such as Social Security numbers or driver's license numbers.
- While we have been closely monitoring these accounts, we have not detected any increased incidences of fraud on these 12,000 accounts. We are continuing to monitor these accounts for any suspicious activity.

According to reports from CyberTrust and other published reports, the intrusion into the CardSystems database was made possible by the failure to have appropriate computer intrusion protection and detection measures in place. This was exacerbated by the storage on CardSystems' database of credit and transaction data that should have been purged from its records, and it was further exacerbated by the failure to encrypt the stored data. Such actions would violate both American Express' data security policies and the PCI Standards.

We take these violations very seriously. Based on our current analysis, we have notified CardSystems of our intention to end the processing relationship with them.

Fraud Detection and Prevention

American Express employs sophisticated monitoring systems and controls to detect and prevent fraudulent activity. Historically, this has been an area of emphasis for American Express. Over the last several years, we have invested tens of millions of dollars to enhance our fraud prevention capabilities to better protect Cardmembers. It is

in our interest to do so, since by minimizing fraud we reduce the considerable costs to us and the industry each year from fraudulent activity. If fraudulent charges are placed on an American Express Card account, we stand behind our Cardmembers. American Express Cardmembers are not held liable for fraudulent charges.

Since 2001, both the transaction volume and charge volume on our network has increased substantially. During this period the overall fraud rate has declined significantly. We are constantly adjusting our fraud prevention techniques to adapt to the changing strategies of fraudsters. While we do not disclose the details of our fraud prevention measures in order to prevent criminals from having knowledge of our procedures, steps we take to protect our Cardmembers include the following:

- Customer Password: Every American Express Cardmember is asked to establish a password in the voice response system, providing an additional level of authentication for account maintenance.
- Charge Verification: On transactions above $200, if fraud is suspected by a merchant, the merchant can contact American Express and we will speak directly with the Cardmember to authenticate the transaction.
- Card Identifier Digits/Card Identification Number (CID): The CID number provides an additional level of verification for merchants (both online and off). This 4-digit number is printed on the front of all American Express Cards (also referred to as CVV2 or CVC2 as a 3 digit number on the back signature panel of bank cards).
- Zip Code Verification: This provides for an additional level of authentication at the point of sale by enabling merchants to ask

Cardmembers to provide their zip code, which may be a piece of information a fraudster would not have.

- Automatic Address Verification (AAV): This verifies for the merchant that the address provided by the customer matches the billing address on file with American Express. Our AAV technology is very sophisticated and is considered a "best practice" in the industry.

In the case of the CardSystems breach, we have implemented additional security and fraud prevention measures for all of the American Express Card accounts with information stored on CardSystems' database. In addition to our normal fraud detection procedures, we continue to closely and more intensely monitor these particular accounts for any suspicious activity on an ongoing basis.

If we detect any unusual activity on these accounts that may be fraud, we will contact the customer. In many instances, we detect fraud well before a customer becomes aware of any unusual activity on an account, and we proactively reach out to affected customers. If we verify with the Cardmember that fraud has occurred we will replace the Card.

If we learn that any merchant, processor, or any other participant in the payment card transaction cycle may have been subject to a breach, we quickly apply additional anti-fraud measures. It is important that we learn about any potential breach promptly so that our additional fraud detection and prevention measures can be implemented as quickly as possible. It is also important to reiterate that American Express Cardmembers are not held liable for any fraudulent charges.

Identity Theft Prevention

It is important to distinguish between two different types of criminal activity: credit card fraud and identity theft. Fraud occurs when a criminal places a fraudulent or unauthorized charge on a card account. Identity theft occurs when a criminal uses information about a person to open a new account in the victim's name or to take over use of an existing account by changing, for instance, the name or billing address on the account. Typically, a criminal needs access to sensitive personal information, such as the date of birth, a driver's license number, or a Social Security number, to commit identity theft. This distinction becomes important when analyzing particular data elements that may have been compromised and the harm to customers that might result from the misuse of compromised information.

In order to help consumers detect and prevent identity theft, American Express provides free Identity Theft Assistance to all American Express Cardmembers. This assistance includes access to representatives who are on call 24 hours a day, seven days a week, to offer help on how to protect against identity theft; it also suggests steps Cardmembers can take if they notice any suspicious activity on their accounts. American Express Cardmembers can also sign up to receive alerts for any irregular account activity, via cell phone, PDA, or e-mail. This alerts program is available at no cost to our Cardmembers.

In addition, American Express has a long history of working externally with consumer and privacy advocate organizations to educate consumers on issues such as information security, fraud and identity theft. Most recently, we hosted a roundtable discussion on identity theft that included participation from the U.S. Department of

Treasury, FBI, FTC, and the Council of Better Business Bureaus. We also published a consumer brochure in cooperation with the California-based Privacy Rights Clearinghouse and the Identity Theft Resource Center on how consumers can protect themselves against identity theft and the steps consumers can take if they become victims. We are also major supporters of the National Consumers League online Fraud Information Center and are active members of the Alliance Against Fraud in Telemarketing and Electronic Commerce.

Later this year, we are co-sponsoring a summit to address the growing problem of "phishing." One concern is that "phishers" will take advantage of known data breaches to send out counterfeit notifications seeking personal sensitive information. Summit participants will include consumer advocates, federal and local law enforcement officials, internet service providers, technology companies and academics. As has been our tradition, we will continue to work in cooperation with consumer advocates to increase consumer awareness of these issues and identify solutions.

Customer Notification

American Express supports a consistent and effective national notification standard as an important component of data security response program. Notification to consumers is appropriate when compromised information is reasonably likely to be misused to the harm of the consumer and the notification will provide the consumer a meaningful opportunity to take appropriate steps to protect against that harm. We believe the current notification regime could be improved by addressing three important areas.

First, there should be an appropriate threshold to trigger notification. The intent of notification is to prevent harm to the customer; over-notification can result in

consumers becoming desensitized to the many notices they might receive. As a result, consumers could pay insufficient attention to a significant incident and fail to act when preventive measures are necessary.

Second, we believe that notification requirements must take into account the scope of the particular information that has been compromised and the harm to consumers that could result from the misuse or potential misuse of compromised information. Notifications are useful to consumers if they communicate the significance and likelihood of the potential harm caused by a breach and provide guidance on how to prevent or mitigate the potential harm. All compromises are cause for concern, but not all compromises present the same potential consequences or potential harm to consumers.

Third, a consistent and effective national standard for notification serves consumers best. It will enable uniform application across the country and lead to uniform enforcement by regulators and law enforcement authorities. It is undesirable and impractical to have a patchwork of consumer notification requirements that vary by state or entity.

Recommendations

In light of these recent data security breaches, we believe there are some tangible steps that can be taken to better protect consumers. First, payment card transactions are handled by regulated and unregulated companies, and we recommend that Congress extend Gramm-Leach-Bliley (GLBA)-like safeguard standards to those companies involved in processing card payments that are not currently subject to these safeguards.

Sensitive customer information should be consistently protected as it proceeds through the payment card transaction cycle. All participants in the payment card

transaction cycle that possess or control sensitive customer information should have a direct legal obligation to implement appropriate data security measures to safeguard that information.

We would also suggest that appropriate cross-industry measures be implemented to certify, and verify on an ongoing basis, adherence to the PCI Standards by all entities in the payment card transaction cycle. This effort should include processes to notify, promptly and simultaneously, all potentially impacted issuers and network providers if a breach is discovered.

We also support increased criminal penalties for those who steal sensitive personal information and those who commit computer fraud. While we recognize that it is often very difficult to catch those who commit this type of fraud, we believe that enhanced criminal penalties would provide law enforcement additional tools to go after fraudsters and is an important step in helping to combat this activity.

The issues discussed here today are complex; appropriately addressing these issues will require dialogue among legislators, regulators, law enforcement agencies and the industry. By working together, we can provide the protection consumers need while maintaining the convenience of using charge and credit cards that consumers have come to rely on.

Conclusion

I want to assure the Subcommittee that American Express is strongly committed to protecting the security of our Cardmembers' personal information. It is clear that recent events have raised the public's concern regarding the security of their personal information, and how this information may be compromised and potentially misused.

We share this concern and are constantly working to protect the security of our Cardmembers' information so that when a customer makes a transaction using an American Express Card, they have confidence that it will occur in a safe and secure manner. Data security is a critical issue for our entire industry, and we are committed to working with all interested parties to ensure a secure payments environment.

We appreciate the opportunity to share our views on this issue, and we look forward to working with you and other members of the Financial Services Committee. This concludes my prepared testimony. I would be happy to answer any questions that you may have.

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Testimony of

Evan Hendricks, Editor/Publisher
Privacy Times
www.privacytimes.com

Before The House Committee On Financial Services
Subcommittee On Oversight & Investigations

July 21, 2005

Madame Chairwoman, thank you for the opportunity to testify before the Subcommittee. My name is Evan Hendricks, Editor & Publisher of Privacy Times, a Washington newsletter since 1981. For the past 25 years, I have studied, reported on and published on a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have served as an expert witness in litigation, and as an expert consultant for government agencies and corporations.

I am the author of the book, "Credit Scores and Credit Reports: How The System Really Works, What You Can Do."

Due to pre-existing travel plans and other commitments, I am not able this time to provide as detailed a prepared statement as normal. Please allow me to make some fundamental points.

The breach of the credit card data of 40 million consumers underscores several important weaknesses in our national privacy policy.

1) Our traditional approach to privacy problems, reacting to anecdotal problems with narrowly tailored legislation has left major gaps in what information is protected, and to what extent it is protected. Credit card processors argue that they are not

covered by the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, or other laws to protect financial privacy.

2) If institutions have discretion not to notify consumers of a breach, some institutions won't notify consumers.

3) Individuals seeking to learn if they're information was compromised cannot always get straight answers from customer services representatives.

4) Breaches impose real costs and damages on consumers, including loss of time, energy and opportunity, and stress

5) Individuals are often left without direct recourse or a remedy, despite the damaging nature of some breaches.

6) For many organizations handling sensitive consumer data, security remains an afterthought.

Loss of Consumer Confidence

Given the nature of recent breaches potentially affecting 50 million Americans, it should be no surprise that consumer confidence in the security of credit card data and other sensitive information is falling. This could have enormous, negative implications for the economy. The conventional response is to fret more about the effect that increased privacy protections will have on the prerogatives of large organizations. This case should show that we've reached a tipping point, where the risk to consumers individually, and the economy as a whole, is too great to put off an aggressive legislative platform for protecting consumer data. Just reflect upon the fall in small investor confidence following the burst of the "dot-com bubble," and more troubling, the accounting scandals of Enron and WorldCom. The current breaches indicate that our financial data systems are heading for a fall in consumer confidence.

FACTA Was Progress, More Is Needed

Thanks in large part to the work of this Committee, the FACT Act represented important progress in expanding more comprehensive protections for consumer privacy. Unfortunately, the recent breaches underscore that more needs to be done.

Starter List For More Progress

Leading lawmakers are working hard on more comprehensive solutions. Many of the efforts are bipartisan. Reps. Frank, Hooley, Barton and others are all working on the issue. Sens. Specter and Leahy are working together at Senate Judiciary Committee. At the Commerce Committee Sens. Gordon Smith and Bill Nelson are working with Sens. Daniel Inouye, John McCain, Mark Pryor and Stevens. One of the more comprehensive measures is the one introduced earlier this year by Sens. Nelson and Schumer.

The challenge is to be able to advance federal legislation that does not preempt State law. Because of recent progress in the states in the areas of breach-notification laws and credit report "freeze" laws, it would be very counterproductive to preempt State laws in these areas.

Here are some of the areas that need to be addressed to restore consumer confidence in the security of their data:

1) Extend to all data brokers and information aggregators the rights of Fair Information Practices (FIPs), including (1) access to and (2) correction of records, (3) purpose specification, (4) collection limitation;
2) Create a private right of action so people have a remedy when they are unreasonably damaged by breaches
3) Restrict the uses of Social Security numbers
4) Create a national standard for breach notification, but only if it improves upon the California law
   a) Require companies responsible for breaches to offer victims free credit monitoring services
   b) Create a federal seal for the outside of the envelope to notify people that the a notice of a data-security breach is inside
5) Extend security safeguards to non-financial institutions
6) Create a national standard for freezing credit reports, but only if it doesn't preempt State law
7) Require more matching of identifiers before a credit report can be disclosed (see California statute)
8) Create a U.S. Privacy Commission to oversee privacy policy, investigate complaints, and advise Congress

I'd be happy to answer any questions. I've attached a related article that I published in the March 6, 2005 *Washington Post.*

www.washingtonpost.com/wp-dyn/articles/A9101-2005Mar5.html

When Your Identity Is Their Commodity

By Evan Hendricks

Sunday, March 6, 2005; Page B01

So you think it's your personal information? That's not the viewpoint of the mega-companies compiling and selling data about you. As they see it, if they collect the information, they own it. Sure, it's about you, but it's theirs. You might think "privacy," but they see a commodity -- and a valuable one at that.

And for now, they're right. Never mind that there's a fundamental conflict built into this arrangement. The same companies entrusted with safekeeping our essential information make money only if they sell that information, and they do so in bulk. What's more, the current system places the burden on you to put a stop to any practices you don't like -- provided you discover them. You have to obtain your credit file, dispute errors, "opt-out," call, write -- and hope for the best.

Those are a few of the lessons emerging from a pair of privacy debacles last month that left millions of Americans asking how they can protect themselves and their data in an age when identity theft is the crime of choice. The first of these fiascos involved a company called ChoicePoint Inc., which admitted that it had been tricked into providing information on 145,000 people to a group of bogus companies, and the second stemmed from Bank of America's loss of credit data on 1.2 million federal employees. The incidents suggest that our sensitive personal information has been treated as just another commodity, deserving no more respect (and maybe less protection) than soybeans or pork bellies.

The scandals have re-stoked congressional interest. The day after Sens. Arlen Specter (R-Pa.) and Patrick Leahy (D-Vt.) announced Judiciary Committee hearings on the ChoicePoint scam, Leahy learned that his credit card data was on the Bank of America backup tape that disappeared without a trace. Like the growing number of Americans victimized by such "leakages," he didn't sound too happy.

Perhaps these events will prove to be the tipping point for policymakers and will educate consumers as to their stake and role in what has been aptly termed the "Data Revolution."

Did we say we wanted this revolution?

In fact, we did -- or at least we didn't complain about its benefits. Without the data revolution, there would be no information age. Personal information is vital to this new epoch. The collection and sharing of that information has powered the economy by increasing the availability of consumer credit, while at the same time lowering the cost of granting it. It also facilitates screening of employees, tenants, nannies and others who are entrusted with access to

offices and homes. It makes it more convenient for our highly mobile population to buy houses, rent apartments and get instant store credit.
But there's a dark side: The current system invites identity theft, a fast-growing and distressing crime.

Ultimately, privacy has a very good chance of prevailing over the forces chipping away at it. Not only do Americans overwhelmingly view privacy as a fundamental right that must be preserved, but the economics of the electronic age also dictate the need for innovations that will protect that personal information while continuing to enable the information age.

Brace yourself, however: it's going to get worse before it gets better.

As the Supreme Court has recognized, the key to protecting privacy in the modern world is ensuring that individuals maintain reasonable control over their personal data. Reaching that goal requires a mix of strong national policy, good use of technology and consumer awareness.

ChoicePoint's recent lapse shows how far we have to go. A still at-large fraud ring became "customers" of ChoicePoint by posing as 50 fake businesses, including debt collectors and check-cashing firms. The thieves used ChoicePoint as a portal for accessing at least one major credit bureau, enabling them to filch Social Security numbers, other identifiers such as addresses, and sensitive credit report data. Although the full extent of the damage is not yet known, it's clearly one of the worst cases ever: ChoicePoint sent letters to 145,000 consumers warning that their data were compromised; 750 individuals were confirmed victims of identity theft.

The perpetrators picked quite a target. ChoicePoint is a symbol of the "commodification" of our personal data, having compiled 19 billion records covering virtually every American adult. A spinoff of Equifax, the giant credit bureau, ChoicePoint taps a wide range of taxpayer-subsidized sources, including local property records; driver records; boating, pilot and professional licenses; and court records showing bankruptcies, liens, judgments and divorce. Its sales to corporations and governments last year topped $900 million. (Other database companies are Acxiom, LexisNexis, Westlaw and Seisint.) While some of ChoicePoint's mammoth databases are filled with public records, these records are no longer "public" once ChoicePoint houses them. The company will give you access to some of the files it keeps on you, as required by the Fair Credit Reporting Act (FCRA). But it recently argued to the Electronic Privacy Information Center (EPIC), a public interest research center here in Washington, that other data are not subject to the FCRA.

That means you cannot see your data or correct errors -- even though other companies and government agencies could buy the same data and use them for making decisions about you.

With the Byzantine nature of the laws governing personal information and of the electronic systems that house such information, you need a scorecard to know when your information is protected by federal statute: credit reports (yes), video rental records (yes), federal agency records (yes), medical records (generally no), bank and credit card records (kind of), non-credit database company records (who knows?).

Our system evolved this way because Congress has declined to take a comprehensive approach that would establish a baseline of protection for all personal information. Instead, it has focused on some sectors, or responded to problems as they have arisen.

Congressional action became imperative after the Supreme Court ruled in 1976 that the Constitution did not protect personal data held by banks and other private firms. In essence, the court held that by becoming a bank customer, you surrender your information to the flow of commerce, and thereby surrender your privacy. The information might be about you, but if financial institutions collect and keep it, they own it.

So yes, your information is a commodity; and no, you don't get a cut.

The credit report is at the epicenter of identity theft. First it enables the crime and later it becomes the main source of damage to the victim.

There are three major credit reporting agencies (CRAs) -- Equifax, TransUnion and Experian (formerly TRW). Each maintains electronic credit reports on 200 million American adults. The industry proudly proclaims the system as the best in the world, and claims it has boosted the economy by reducing the cost of credit while increasing convenience for businesses and highly mobile consumers.

Throughout the 1990s, however, complaints about glaring inaccuracies and the CRAs' inability, or unwillingness, to correct them prompted Congress to act. In 1996, it strengthened the first privacy law, the Fair Credit Reporting Act of 1970. Burgeoning identity theft led to more FCRA amendments in 2003.

We know why Willie Sutton robbed banks. Identity thieves also know where the money is. Once they steal identities, thieves can get credit in the victim's name and go on a shopping spree.

When a thief applies for credit using your name and Social Security number (SSN), the CRAs disclose your credit report. Typically, their algorithms will tolerate conspicuous discrepancies in name and address, even in city and state, as long as the fraudster puts your exact SSN on the credit application. It turns out to be a relatively low-risk, high-reward crime.

A Federal Trade Commission survey estimated that nearly 10 million Americans were victims of some form of identity theft in 2003, triple the number in 2001. Yet, in a little-noticed report that year, the TowerGroup, a Massachusetts-based consulting firm, said the incidence of identity theft was such a small fraction of transactions that most financial service companies could not justify the extra expense of preventing it.

That's not much comfort to the victims who describe such crimes as a form of "data rape" that leaves them deeply scarred. It takes a maddening amount of time and effort to persuade credit bureaus to remove fraudulent accounts from credit reports, or to convince creditors to stop reporting them. In the meantime, unpaid debts and collections can ruin a victim's credit score, often leading to denials of mortgages or other credit. The aggravation and frustration tend to

compound. The burden is on the victim to write certified letters, keep records and follow up until the problem is solved.

How can you protect yourself? It's ironic, but the best method of protection is regularly checking your own credit report for early signs of identity theft. The report shows which companies have pulled it and why. So if you live in Virginia and a car dealer in Texas pulled your report -- that's a red flag. Another sign is an unpaid debt that isn't yours. Starting Sept. 1, East Coast residents can get all three of their credit reports once a year for free -- thanks to Congress's 2003 overhaul of the FCRA. Marylanders already are entitled under state law.

To its credit, ChoicePoint is offering free credit reports and a free report-monitoring service to the 145,000 recipients of its warning letter. Monitoring services offer a glimmer of hope, as they give you regular access to your credit report and alert you to new entries. Such alerts could enable you to nip identity theft in the bud. The main problem is that each credit bureau charges about $100 a year for the service. It's a bit like a protection racket. They will charge you so you can make sure that they did not improperly divulge data to help an identity thief. That's good work if you can get it.

Since the FCRA already requires "maximum possible accuracy," and directs bureaus to curb identity theft, why aren't such services "standard features," rather than "extras"?
Price aside, these services prove a vital point: Database technology has finally allowed us to plug into our own personal information, a privilege thus far reserved for the CRAs and ChoicePoints of the world -- and the thousands of companies they sell to. This will enable individuals to ensure the accuracy and proper use of their data, and to promptly rap the knuckles of those who cross the line.

The information age, understandably viewed as detrimental to privacy, can be turned to privacy's advantage. In the future, all individuals will routinely monitor their personal data, and not just their credit reports. The companies that now seem to be the crux of the problem have incentives to make us all part of the solution. Government agencies and major corporations can save billions of dollars by converting personal data transactions from paper to electronics, but public resistance will continue until there's a strong privacy regime in place. The ChoicePoints of the world could even profit by helping, but they'll have to view us as more than just "data subjects." It's ironic that large firms, which have been careless about privacy, might discover they have financial incentives to become genuine privacy advocates, and figure out ways to live up to the task. Of course, that realization is probably a ways off.
Meanwhile, go check your credit report.

Author's e-mail: evan@privacytimes.com

Evan Hendricks is editor and publisher of Privacy Times and author of "Credit Scores & Credit Reports: How the System Really Works, What You Can Do" (Privacy Times).

Statement of

Carlos Minetti

Discover Financial Services

Before the

Subcommittee on Oversight and Investigations

of the

Committee on Financial Services

United States House of Representatives

July 21, 2005

Madam Chairman and Members of the Subcommittee, thank you for inviting Discover Financial Services[1] to share our views on the issue of data security breaches affecting credit card information.

As Discover's Executive Vice President for Cardmember Services, I am responsible for operations, customer service and risk management. This includes oversight of Discover's information security and anti-fraud efforts.

---

[1] Discover Financial Services, Inc., headquartered in Riverwoods, IL, is a business unit of Morgan Stanley. It operates the Discover Card with more than 50 million Cardmembers, the Discover Network with more than 4 million merchant and cash access locations and the PULSE ATM/Debit network currently serving more than 4,000 banks, credit unions and savings institutions.

The subject of today's hearing – the security of financial information - is very important to financial services providers and the consumers we serve. Security breaches and the appropriate responses to them are issues that must be addressed in a consistent manner so that consumers nationwide have the same protections and confidence in the security of their financial information no matter where they live.

Security Breach Prevention

Discover works hard every day to prevent customer information from falling into the hands of individuals who would hope to use it for criminal purposes, like account fraud or identity theft. Identity theft involves unauthorized use of personal information (such as an individual's name, address and Social Security number) to open *new* accounts with financial institutions or other service providers in the name of the victim, but without the knowledge of the victim. Identity theft can result in frustrating efforts to reclaim one's identity and other costly consequences.

Account fraud, on the other hand, involves the use of an *existing* credit card without authorization of the cardholder to make purchases or obtain cash advances. The real victim of this crime is generally not the consumer whose account was involved, but rather the credit card issuer. Federal law limits consumers' responsibility for unauthorized transactions (Discover customers' liability for fraudulent transactions is zero), and consumers can generally have these transactions erased from their accounts with little difficulty.

At Discover, we continually review, and if necessary upgrade, internal efforts to ensure that access to information is limited to individuals who have a legitimate business need to see it; that employees are adequately screened, trained and monitored; that computerized information is maintained securely; that the identity of card applicants is verified; and that customer accounts are monitored for signs of suspicious activity. Financial institutions, like Discover Bank, the issuer of our cards, are subject to the Gramm-Leach-Bliley Act's information security standards and the Interagency Guidance on security breach response programs. The FDIC examines Discover Bank for compliance with those standards.

Protection of Discover Cardmembers

Discover monitors its 50 million Discover Cardmember accounts nationwide for signs of unauthorized activity, and notifies Cardmembers in the event of suspected account misuse. We provide Cardmembers with information and educational messages about safeguarding personal information and with tools to enhance the security of that information.[2] Our Customer Service Representatives are available 24 hours a day, every day, to assist all Discover Cardmembers with inquiries or concerns about information security and to resolve issues about unauthorized transactions promptly. These representatives are empowered to address customer inquiries expeditiously, without

[2] For example, Cardmembers who shop over the Internet can use Discover's secure online shopping service that generates a single-use card number to be used in lieu of the Discover Card account number.

requiring the customer to make multiple calls, navigate through menus of options, or listen to lengthy recorded messages.

In the event that a consumer believes that he or she is a victim of identity theft involving a Discover account, we assign a Personal Fraud Specialist to assist the individual in working with creditors, law enforcement personnel, and consumer reporting agencies. Consumers appreciate the ability to stay in contact with the same Specialist throughout the process of resolving identity theft issues.

A 2005 "Identity Fraud Safety Scorecard for Credit Card Issuers" conducted by Javelin Strategy & Research ranked Discover first in "overall card safety features" and first for "detection safety features." [3]

Data Held by Merchants, Their Processors and Other Service Providers

As Discover and other credit card issuers and networks improve internal defenses against computer hacking and other threats to the information we hold, criminal enterprises have begun to focus on what they may see as "soft targets." These include merchants and service providers that accept credit cards, and the third party vendors that they use to process payment information and manage their businesses.

[3] 2005 Issuer Scorecard" by Javelin Strategy & Research (www.javelinstrategy.com). Javelin's study scored issuers on 38 categories of capabilities for fraud prevention, detection and resolution.

The millions of businesses that accept credit card payments include the largest American companies that accept cards for billions of dollars in sales and account for a significant volume of total retail sales (and credit card transactions). The largest merchants are the most attractive targets for would-be identity thieves or fraudsters, but they also tend to have the most sophisticated information processing systems and data protection regimes, backed up by internal security teams. Cards are also accepted by millions of smaller entities, some of them part-time businesses operated by a single individual. Although smaller merchants may not have similar information security systems or resources, they are also less likely to be targeted by large scale ID theft or fraud rings because the volume of data they hold may simply not be worth the effort involved in stealing it. In evaluating the adequacy of efforts to safeguard personal financial information held by merchants and service providers, it is important to be mindful of these differences, so that resources are allocated appropriately and unnecessary and unworkable approaches are avoided.

Discover's contracts with the merchants that accept Discover Network cards requires them to safeguard account information, and to use it only for specified purposes related to payment processing. The merchants agree that they will not store the full information encoded in a card's magnetic stripe or the three-digit card validation code, and that they will destroy or purge obsolete transaction data. Merchants also commit to providing access to the data only to processors, software vendors, and other agents or service providers that have security standards that comply with these requirements.

The Discover Network has direct relationships with each of the merchants and service providers who accept Discover Network cards. Discover communicates regularly with these merchants to remind them about our data security requirements, inform them about emerging threats and software or other vulnerabilities, and provide information about resources and technical assistance for enhancing data security. Discover provides its merchants with tools and services that can be used to validate their compliance with our requirements for secure information processing and transmission. For online merchants, who are particularly vulnerable to security breaches, our Merchant Operating Regulations give the Discover Network the right to perform periodic data security scans to ensure that the merchant remains in compliance with Discover's security and encryption requirements.

Discover reviews merchant and processor data daily. This helps to pinpoint areas of vulnerability by identifying suspicious transactions and patterns of activity. It is a risk-based approach that allows us to focus compliance efforts where they are needed, and is the basis for identifying merchants or processors for targeted responses in the form of alerts and inquiries, transaction monitoring, and physical audits.

Discover's security requirements, which we revised in 2004, are consistent with the "Payment Card Industry Data Security Standard." This is an industry-wide standard for the protection of account data that allows merchants to use the same procedures regardless of the cards they accept or the processors and agents they use. It also allows

merchants to use a single set of security standards in assessing the adequacy of their efforts to safeguard information about their customers' payment card transactions.

Discover's Security Breach Response Measures

Discover's response to data breaches are consistent with standards specified in the Interagency Guidance on Response Programs and a growing number of state laws. We also have a strong financial interest in addressing security breaches, because as noted previously Discover, and not our Cardmembers, absorbs the losses from fraudulent transactions. When information obtained by virtue of a data breach is used to make purchases or cash withdrawals on a Discover account, we promptly delete the charge from the account and absorb the loss.[4]

Because we operate both a large merchant network and issue the Discover Card, we are often able to learn about computer hackings and other signs of data compromises when they first occur. In fact, Discover was the first network to uncover evidence of data compromises in many of the recently publicized security breaches involving large merchants and payment processors.

[4] The notion that card issuers are not concerned about data breaches because the chargeback process insulates them from financial loss is simply untrue. We do not routinely charge back purchases to merchants who accept a stolen or counterfeit card or process a transaction not authorized by the cardholder unless the merchant fails to follow card authentication procedures (e.g., obtaining the three-digit security code for online or telephone transactions where no card is presented).

An internal Discover Task Force is responsible for maintaining effective procedures for addressing security breaches. Comprised of individuals from both our card issuing and payment network businesses, the Task Force meets regularly to discuss security issues, and is convened in the event of a breach to assess the appropriate responses. It has developed response action plans to address different forms of data compromise. The Task Force is also responsible for the development of customer education information regarding account fraud and identity theft.

Upon learning of a data security breach that may affect Discover Cardmembers (such as the incident involving credit card data held by CardSystems Solutions, Inc.), we immediately commence an investigation. We first ascertain the type of information involved to determine whether the data could be used to commit identity theft or otherwise harm the customer. For example, did the incident involve unauthorized access to account numbers? account numbers and security codes? customer names and addresses? Social Security numbers? We also identify the specific accounts that were affected, information that we need to monitor those accounts and take further action if necessary, such as contacting our customers or closing accounts.

Where the breach is external (e.g., data held by merchant or processor) we must rely on information from the affected companies. We work with these companies and with third party investigators to evaluate the impact on Discover Cardmembers. We gather information and assist the entity whose security was compromised in retaining (and sometimes in paying for) the services of forensic investigative firms that specialize in

evaluating data breaches. We also work with other card networks when their account data is affected.

If we determine that the data that was accessed without authorization is likely to result in customer harm, we notify affected Cardmembers in accordance with the Interagency Guidance and the requirements of state laws. We also take further actions that may be necessary to prevent harm, such as further monitoring or the closing of accounts.[5] Discover coordinates its efforts with the FDIC and with law enforcement personnel who may be investigating the incident.

Data security breaches do not necessarily expose the consumer to ID theft or even to account fraud. In some instances, the breach may be the work of a hacker who had no criminal intent, or involve encrypted or incomplete information of no value to a criminal. Where the breach resulted in account fraud, protection of the consumer may require no more than account monitoring and the removal of unauthorized charges.

Nevertheless, some industry observers have suggested that credit card issuers should notify all customers and possibly reissue cards in every case in which any potential risk is found (even if the incident can not be verified or the consumers affected can not be validated). They also propose that consumers receive other assistance such as free credit report monitoring. These observers assume that the industry is resistant to such

[5] Account closure and the establishment replacement accounts is often unnecessary and entails costs that exceed the benefits. Where account closure is warranted, Discover facilitates the process. For example, preauthorized payment requests are automatically transferred to the new account so the customer does not have to contact the merchant or service provider and furnish the new account number.

requirements purely due to the cost involved. Given the fact that potential fraud-related losses are incurred by credit card issuers (not by consumers) and since actual fraud losses can quickly eclipse the cost of notification and/or card re-issuance, the cost of notification/re-issuance is generally not the driving factor for decisions about how best to react to a given situation.

Discover carefully weighs all relevant facts and impacts on our customers to determine the proper course of action (obviously complying with all relevant legal requirements). No purpose is served by notifying consumers who are not at actual risk of identity theft about data breaches if the consumer does not need to act to protect his or her information or avoid costs. Likewise there is no need to re-issue cards on accounts that have very low fraud risk. This provides no consumer benefit, but rather may cause inconvenience to consumers who have to activate their new cards and revise their numbers with all "recurring bills" (such as Internet, utility, and health care vendors) to avoid rejected transactions and potential lapse of service.

Of course, after-the fact notification, card re-issuance or other remedies do nothing to address the root cause of a given problem – identity theft. Prevention of data breaches and protection of information should be the primary focus of industry, regulators and the law.

Following the resolution of a data security incident, Discover's data breach Task Force reviews the situation and Discover's response to it to determine if changes are needed to

respond better to future incidents. The development of effective response initiatives is an evolutionary process due to changes in the threats we face. As criminals involved in identity theft become more sophisticated and nimble, we must respond accordingly.

CardSystems Solutions Data Breach

In response to the breach of credit card information held by CardSystems Solutions, we followed the procedures that I have described. The investigation of the incident is ongoing. But based on what we know today, it does not appear that Discover Cardmembers were exposed to a risk of identity theft as a result of CardSystem's loss of Discover data. And while the CardSystems breach *did* involve a loss of Discover data that could be used to commit account fraud, Discover Cardmembers will not experience financial loss as a result of this incident.

These conclusions are based on two facts. First, the Discover information involved in the CardSystems incident was limited to purchase transaction data. This information would not be useful to an identity thief in opening accounts with other financial institutions or otherwise taking over the identity of a Discover customer. Second, to the extent that the criminals involved in the CardSystems breach are able to use the information or make unauthorized transactions on some Discover accounts, our zero dollar fraud liability policy protects Cardmembers from financial loss. Our one-stop, 24/7, customer service program expedites the removal of unauthorized transactions from customer accounts.

Legislative Considerations

1. A national standard for responding to security breaches affecting personal financial information is appropriate. Criminals seeking access to consumer financial information rarely target residents of a single state: large-scale breaches potentially affect individuals across the country. Investigation, reporting, notification and remediation requirements that vary depending on the residence of an individual customer are more likely to impede than facilitate appropriate and prompt responses. National uniformity is needed. Legislation addressing security breach prevention or responses should preempt state laws addressing this subject.

2. For information held by financial institutions, we believe that the Interagency Guidance, coupled with on-site compliance examinations, establishes an effective and proper regime. It also provides regulators with the flexibility they need to adjust breach response standards over time as security threats evolve and the ability to prevent or react to them changes due to technological improvements and enhanced surveillance techniques.

3. Congress is considering proposed data protection and data breach legislation for unregulated entities that hold or process consumer financial information, but are not directly subject to statutory requirements. Coverage of such entities would be analogous to laws requiring merchants to protect customers (and payment card issuers) by suppressing or truncating credit card account numbers that are printed on sales receipts.

If Congress concludes that such broader security breach legislation is appropriate, the Interagency Guidance provides a good model for appropriate definitions, a consumer notice triggering mechanism, and response standards.

4. Finally, in the event of a data breach affecting credit card information, notification is best handled by the card issuer, not the entity whose security was breached. That entity whose security was compromised must cooperate fully in providing the details necessary to ensure efficient response and notification by the issuer, and to prevent further fraud. But requiring merchants or processors to directly notify affected cardholders may impose an obligation that they cannot readily achieve (since they may not have the necessary consumer contact information), and can needlessly alarm individuals who were not adversely affected by the breach. This might encourage consumers to take steps that are unnecessary (e.g., closing accounts, placing fraud alerts on credit reports). A single notice is the best way to protect credit card users, and card issuers are in the best position to determine whether and when that notice is appropriate.

Conclusion

Discover Financial Services appreciates the opportunity to discuss information security issues with the Subcommittee. We would be pleased to provide further information that would be useful to the Subcommittee in assessing the scope of the problem and the adequacy of current safeguards and response measures.

CREDIT CARD DATA PROCESSING: HOW SECURE IS IT?

TESTIMONY OF JOSHUA L. PEIREZ
SENIOR VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL
MASTERCARD INTERNATIONAL

Before the Subcommittee on Oversight and Investigations of the
House Financial Services Committee

July 21, 2005

Good morning Chairwoman Kelly, Congressman Gutierrez, and members of the Subcommittee. My name is Joshua Peirez and I am a Senior Vice President and Associate General Counsel at MasterCard International in Purchase, New York. It is my pleasure to appear before you this morning to discuss the important topic of information security and I commend the Committee for holding this hearing. MasterCard is a global organization comprised of more than 23,000 financial institutions that are licensed to use the MasterCard service marks in connection with a variety of payments systems. It is important to note that MasterCard itself does not issue payment cards nor does it contract with merchants to accept those cards. Instead, those functions are performed by our customer financial institutions. The financial institutions that issue payment cards bearing the MasterCard brands are referred to as "card issuers." The financial institutions that enter into contracts with merchants to accept MasterCard-branded cards are referred to as "acquirers." MasterCard provides the networks through which the customer financial institutions interact to complete payment transactions and sets the rules regarding those interactions.

MasterCard takes its obligations to protect MasterCard cardholders, prevent fraud, and safeguard financial information very seriously. In fact, this issue is a top priority for us, and we have a team of experts devoted to maintaining the integrity and security of our payment systems. We are also proud of our strong record of working closely with federal, state, and local law enforcement agencies to apprehend fraudulent actors and other criminals. Included among the federal law enforcement agencies with which we work closely are the U.S. Secret Service, the U.S. Department of Justice (including the Federal Bureau of Investigation), the Federal Trade Commission, the U.S. Postal Inspection Service, and others. MasterCard also fields calls from local law enforcement regularly. MasterCard believes its success in fighting fraud is perhaps best demonstrated by noting that our fraud rates are at historically low levels, well less than one-tenth of one percent of our volumes.

Information Security

Our success in protecting consumers and thwarting fraud is due in part to the constant efforts we undertake to keep our networks secure. The MasterCard information security program is robust, and we continually update it to ensure that security remains strong. Our customer

financial institutions also have information security protections in place including those required under applicable banking law, such as the Gramm-Leach-Bliley Act (GLBA). For example, here in the U.S. our customer financial institutions must adopt a comprehensive written information security program to protect their customers' personal information that includes administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These safeguards must be approved and overseen by the customer financial institutions' board of directors. The safeguards must include an assessment of risk, procedures to manage and control risk, the oversight of service provider arrangements, and a mechanism to monitor and adjust the written information security program as necessary.

MasterCard also requires its customer financial institutions to adhere to a comprehensive set of rules established by MasterCard to ensure the integrity and safety of MasterCard's payment system. For example, MasterCard's bylaws and rules require each customer financial institution, and any third party acting on behalf of such customer, to safeguard transaction and account information. Not only must our customer institutions safeguard MasterCard transaction and account information, but our bylaws and rules require any merchant that accepts a MasterCard-branded payment device to prevent unauthorized access to, or disclosure of, account, cardholder, or transaction information.

MasterCard, along with other participants in the payment card industry, has also adopted the Payment Card Industry Data Security Requirements ("PCI Standards"). The PCI Standards apply to all customer financial institutions, merchants, and service providers that store, process, or transmit cardholder data. Compliance with the PCI Standards is mandatory as of June 30, 2005. The PCI Standards are comprised of twelve general requirements designed to: (i) build and maintain a secure network; (ii) protect cardholder data; (iii) ensure the maintenance of vulnerability management programs; (iv) implement strong access control measures; (v) regularly monitor and test networks; and (vi) ensure the maintenance of information security policies. For example, not only must our customer banks have comprehensive data security controls in place, but so must the merchants and service providers with which they contract. If a customer bank, or its merchants or service providers, fail to comply with the PCI Standards, the customer bank can be subject to significant penalties. In addition, MasterCard offers a multi-tiered, comprehensive set of global security services designed to help protect participants in our system from hack and attack. MasterCard designed these services to be a cost-effective diagnostic tool to allow participants to understand any systems vulnerabilities they may have. Furthermore, MasterCard also recommends actions that can be taken to reduce the potential systems vulnerabilities.

Consumer Protection and Fraud Prevention

In addition to the strong information security programs in place, MasterCard remains constantly vigilant in an effort to detect potential data breaches or other potential fraudulent activity in order to mitigate any damage. MasterCard has an array of consumer fraud protections and anti-fraud tools, which are publicly available to merchants and consumers, some of which I would like to describe.

Zero Liability and "Chargeback" Protection

First and foremost, MasterCard has taken steps to ensure that MasterCard cardholders are not responsible for fraudulent activity on their U.S.-issued MasterCard consumer cards. In fact, we believe that our cardholder protections are among the most important consumer benefits a cardholder has as these benefits provide consumers with the security and comfort necessary to make the MasterCard system "the best way to pay for everything that matters." For example, MasterCard has voluntarily implemented a "zero liability" policy with respect to the unauthorized use of U.S.-issued MasterCard consumer cards. It is important to note that MasterCard's protection with respect to zero liability is superior to that required by law. Specifically, the Truth In Lending Act imposes a $50 liability limit for the unauthorized use of a credit card. Under the Electronic Fund Transfer Act a cardholder's liability for unauthorized use of a debit card can be higher. However, MasterCard provides all U.S. MasterCard consumer cardholders with even more protection. Under our rules, a cardholder victimized by unauthorized use generally will not be liable for any losses at all. This has greatly enhanced consumer confidence, including with respect to shopping on-line. A MasterCard cardholder can shop with the confidence that he or she will have no liability in the event that his or her account number is used without authorization.

Cardholders who use MasterCard cards also gain additional protections against merchants who do not perform as expected. In many instances, if a cardholder uses his or her MasterCard card to pay for a product or service, and the merchant does not provide the product or service as promised, the issuer can "chargeback" the transaction and thereby afford its cardholder a refund. This is a valuable consumer protection that is obviously not available with other forms of payment such as cash, checks, or travelers checks.

Card Security Features and Address Verification Service

MasterCard payment cards have significant security features designed to prevent criminals from counterfeiting our cards. For example, MasterCard cards have a highly sophisticated hologram. Our research suggests that this is not simple to duplicate in a credible manner. Furthermore, our cards include a magnetic stripe on the back. Not only does the magnetic stripe include such essential data as the payment card number, but it also includes additional information used to verify the card's genuine issuance. The back of the card also includes a specialized signature panel with numbers engraved into it, making it more difficult to reproduce. Of course, issuers also add security features to the card, such as photographs of the cardholder or distinctive graphics and card designs.

We have also provided security features in the event a criminal obtains a cardholder's account number. It would seem ironic to say this, but MasterCard has worked to ensure that the account numbers alone on a MasterCard payment card do not hold much value. By this I mean that MasterCard has several systems in place to thwart a criminal who steals an account number, but steals little else. For example, it seems obvious but it is worth noting that if a thief fraudulently obtains a cardholder's account number, he or she would have a difficult time walking into a merchant to make a purchase because the thief would not have the card itself to present to the cashier.

MasterCard has worked hard to make it just as difficult for a criminal to make use of a card number in transactions where the card is not present, such as in telephone, mail, or Internet transactions. One tool to ensure that the person presenting the number is actually the cardholder is the added security features on the back of the card. MasterCard cards have the last four digits of the account number printed on the back of the payment card, with an additional three digits which do not appear on the front of the card. Many phone, mail, and Internet merchants now request these additional three digits as part of the consumer's payment transaction. In this regard, these three digits can be used to ensure that the person presenting the card number actually has possession of the card—not just the account number.

A tool to fight similar fraud is MasterCard's Address Verification Service (AVS). A criminal who obtains access to a MasterCard account number is unlikely to know the billing address of the individual who holds the account. MasterCard has developed its AVS to take advantage of this fact and prevent the criminal from using the account number. Merchants accepting a MasterCard account number by phone, mail, or Internet are increasingly using AVS as a resource and are asking for the consumer's billing address. At the time of payment, the merchant submits a portion of the billing address into the MasterCard system to verify with the card issuer that the billing address match the account number provided. If AVS indicates that the billing address and the account number do not match, the merchant can take additional steps to verify that the person presenting the number is the legitimate cardholder, or the merchant may simply decline the transaction.

MasterCard SecureCode

MasterCard has developed a service that provides added security when cardholders shop on-line. A cardholder registers his or her MasterCard card with the issuer and creates a private SecureCode. Each time the cardholder makes a purchase at a participating merchant, a box will automatically pop up asking the consumer for the SecureCode—similar to the way an ATM will ask for a PIN when withdrawing money. By correctly entering the SecureCode during an on-line purchase at a participating merchant, the cardholder confirms that he or she is the authorized cardholder. If the correct SecureCode is not entered, the purchase will be declined.

"SAFE" (System to Avoid Fraud Effectively)

MasterCard's System to Avoid Fraud Effectively (SAFE) program is a multi-purpose tool to thwart fraud. The SAFE program is built with the use of data provided by issuers of MasterCard regarding fraud-related transaction information. The SAFE program allows MasterCard to identify fraud at merchant locations and allows us to better focus our global merchant auditing programs. The SAFE program also allows us to analyze certain trends. As just one example, MasterCard may identify countries where certain types of fraud may be unusually high. MasterCard and our customer financial institutions use this data to take the appropriate precautions or otherwise react to the trends as necessary. The SAFE program also helps us to identify potentially fraudulent actors relatively early in the process, before the problem escalates.

Transaction Monitoring

In addition to the proactive protections provided to prevent fraud from occurring, MasterCard and our acquirers have also implemented mechanisms to monitor transactions for potential fraud. For example, MasterCard's systems monitor transaction activity for signs of potential fraud, such as through monitoring merchant or cardholder transaction volume, the incidents of chargebacks, or other unusual activity. We often use this information to pinpoint suspected fraudulent activity so that merchants and banks can take the appropriate precautions.

MasterCard Alerts

One mechanism to place banks on notice is called MasterCard Alerts. MasterCard has developed a reliable and efficient system to notify the appropriate card issuers when MasterCard determines that MasterCard account numbers may have been compromised (*e.g.* fraudulently obtained by others). For example, if MasterCard learns that a card number may have been compromised, it will determine which bank issued the card bearing that account number and will notify the issuer that the account may be compromised. We have the capability to disseminate large numbers of account numbers to issuers in a short period of time through MasterCard Alerts. The issuer has the option to determine how best to address the problem, which may include increased monitoring of the affected account's activities to determine whether the account is being used fraudulently, canceling the account and reissuing a new card and account number to the consumer, or perhaps notifying the cardholder. MasterCard also assists the issuer in monitoring the account usage in order to detect patterns of fraud.

Issuers Clearinghouse Service

MasterCard requires its customer financial institutions in the U.S. to participate in the Issuers Clearinghouse Service (ICS), a system built by MasterCard and Visa using data provided by card issuers regarding, among other things, the fraudulent use of consumer data. More specifically, MasterCard's U.S. customer institutions provide ICS with data regarding customer addresses, phone numbers, and social security numbers that have been associated with fraudulent activity. Furthermore, MasterCard customer financial institutions are required to access ICS in connection with each application to open a MasterCard account. The ICS database allows MasterCard and its customers to detect suspicious activity and to prevent consumer harms, such as identity theft. For example, the centralized ICS database would allow MasterCard and its customers to notice whether a particular social security number was used to open a number of accounts using different addresses. Such activity may indicate that the social security number is being used in a fraudulent manner. MasterCard customer institutions would be provided this data if they received an application with the same social security number or address and the customer institution could evaluate it and take appropriate action.

The CardSystems Situation

I have described some of MasterCard's efforts to fight fraud and keep our systems secure. I would now like to discuss how we addressed the situation with CardSystems Solutions when it occurred. Several months ago, MasterCard and a few of our issuers noticed a small cluster of fraud which had no discernable source. As a clear pattern developed, MasterCard's security

team, working with issuers, was able to identify certain merchants as the source. These merchants shared a similar acquirer. MasterCard, working with the merchants' acquirer, was ultimately able to trace the pattern to a particular third party processor the acquirer utilized, CardSystems Solutions. Based on these factors, MasterCard required CardSystems' acquirer, Merrick Bank, to engage a MasterCard-approved data security firm to conduct a forensic analysis at CardSystems.

Upon being notified of the situation, CardSystems identified the presence of a malicious computer script in its system. The script was designed to export cardholder data without authorization. The Federal Bureau of Investigation was then contacted by CardSystems. Subsequently, the outside data security firm performed a forensic audit. The forensic investigation determined that (1) CardSystems was storing transaction information on its systems in violation of MasterCard rules; (2) there was a computer script found on one of CardSystems' systems, along with other serious security vulnerabilities; and (3) the forensic analysis uncovered specific evidence of a security breach of CardSystems' computer network. The preliminary results of the forensic audit were provided to the acquirer and to MasterCard in mid-June. Final results were provided in July. Based on these findings, it appears that information regarding approximately 68,000 different MasterCard payment card accounts and well over 100,000 payment card accounts of other brands had been exported from the CardSystems database.

MasterCard received a file of the affected account numbers on June 16. Following our established procedure, we used the MasterCard Alerts process to notify the banks affected as quickly as possible, which in this case began the very next day and was completed by Saturday, June 18. We also are working with our customer banks to monitor the potentially affected accounts to determine what additional steps, if any, are necessary. Given the circumstances of this case, MasterCard made the decision that a public disclosure of the event was warranted. Thus, we issued a press release to notify the public of the situation at CardSystems on June 17. I would like to stress that we provided broad public disclosure because it was the only responsible thing to do—not because we had a legal obligation to do so.

As demonstrated by our public announcement, our priority with respect to the CardSystems situation is to protect cardholders. With this in mind, we are now focusing our efforts on ensuring compliance with our data security requirements. For example, we recently sent letters to registered third party processors participating in our system reminding them of their need to comply with MasterCard's rules. Furthermore, we have required certification from the recipients of the letter that they have examined their systems and that such systems do not store sensitive cardholder information. We have also required CardSystems to bring its systems into compliance with our security requirements by August 31, 2005. We are holding weekly meetings with CardSystems to monitor its progress. If, however, CardSystems cannot demonstrate that they are in compliance by August 31, 2005, its ability to provide services to MasterCard customers will be at risk. Of course, we are considering penalties to be assessed with respect to the CardSystems breach as well.

Issuer Reimbursement

We understand the costs to consumers and to our card issuers associated with compromises of cardholder information. As I explained above, MasterCard has programs in

effect to ensure that U.S. cardholders are not liable for fraudulent transactions. MasterCard also has established a program under which our card issuers can obtain reimbursement for the monitoring and reissuance of cards as a result of a security breach.

Legislative Issues

We believe that Congress has established a solid framework for addressing issues relating to data protection. Based on our experience, we urge Congress to consider three improvements to law. First, we believe that stronger criminal penalties and more specific prohibitions should be provided for those criminals who compromise, or attempt to compromise, sensitive personal information. Second, we would like to work with Congress in establishing an appropriate consumer notification mechanism in situations where a data breach poses actual significant risks to consumers. Third, we believe that the law should establish clear data protection requirements for entities in possession of sensitive personal information if such entities are not already covered under the Gramm-Leach-Bliley Act. MasterCard looks forward to working with you as you tackle these important issues.

Conclusion

MasterCard continually strives to provide its customer financial institutions and cardholders with strong protections against fraud and similar activity. These protections include strong information security programs, comprehensive anti-fraud measures, and complete consumer liability protections. Although we are proud of our efforts to protect cardholders, customer financial institutions, and our payment systems against fraud, we will continue to develop new strategies and tools to thwart those who seek to do harm. Furthermore, we will continue to work hand in hand with law enforcement to apprehend perpetrators and continue to make MasterCard payment cards the best—and safest—way to pay for "everything that matters."

STATEMENT OF

JOHN M. PERRY
PRESIDENT AND CEO

CARDSYSTEMS SOLUTIONS, INC.

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON OVERSIGHT
AND INVESTIGATIONS OF THE
COMMITTEE ON FINANCIAL SERVICES

HEARING ON
"CREDIT CARD DATA PROCESSING:
HOW SECURE IS IT?"

WASHINGTON, D.C.

JULY 21, 2005

Written Testimony of John M. Perry
CardSystems Solutions, Inc.
July 21, 2005

Good morning Madame Chairman and Members of the Subcommittee. Thank you for inviting CardSystems to appear before you today. My name is John Perry, and as President and CEO of CardSystems, I welcome the opportunity to discuss the issue of data security. More specifically, CardSystems believes this hearing will help inform the panel, cardholders and the public at large about the facts concerning the security incident perpetrated against us.

First and foremost, we truly regret this occurrence of data theft. We have repeatedly acknowledged our error, and are committed to making sure it does not happen again. As I will discuss in some detail, CardSystems has been working virtually non-stop since this incident, both to thoroughly diagnose what went wrong and to do whatever it takes to prevent any recurrence of this problem.

Make no mistake: exposure of information about one card is one too many. We will not be satisfied until we are confident that everything that can be done has been done to prevent this from happening again.

Despite these efforts, both Visa and American Express have informed CardSystems this week that they both will terminate us as a transactions processor as of October 31, 2005. We are disappointed with these actions and, in light of our diligent efforts to remediate, hope that both Visa and American Express will agree to discuss their decision with us and reconsider, lest we be forced to permanently close our doors.

Introduction

At the outset, let me offer some comfort and assurance to the Subcommittee that we believe what happened to us did not lead to consumer identity theft. The payment card system is designed so that processors like CardSystems do not have access to complete information, such as social security numbers, which could greatly facilitate identity theft.

Turning to the specifics of our situation, CardSystems identified a potential security incident on Sunday, May 22, 2005. Because of the criminal nature of the intrusion, we contacted the FBI on Monday, May 23. On May 25, we notified our sponsor, Merrick Bank.

Immediately after identifying the incident, CardSystems began reviewing all of its systems and hired an independent security firm to assess its operations and to recommend additional security measures. CardSystems has since adopted those recommendations and has installed upgraded security systems to protect them from being targeted again.

CardSystems also has been helping to facilitate all government inquiries, and will continue to do so. These inquiries include those being conducted by the FBI, the FDIC, and the Attorneys General of forty-six of the states, the District of Columbia and three U.S. territories.

Our cooperation with the FDIC includes assisting them in their continuing on-site review at our facilities which began in the third week of June. Also participating in this inquiry at CardSystems' facilities are the Office of Thrift Supervision (OTS), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve.

The State Attorneys General have requested information from CardSystems regarding this incident, with a focus on potential

consumer harm, protection and notification. CardSystems has had multiple discussions with various representatives of the Attorneys General, and has provided and will continue to provide them with information they request as it becomes available to us.

We are still working with the payment card networks, as well as with our customers, who have stood by us as we have investigated this attack on our system. We hope that we may reach a favorable arrangement with Visa and American Express so that we can continue to stay in business.

About CardSystems Solutions, Inc.

CardSystems is headquartered in Atlanta, Georgia and its operating facilities are located in Tucson, Arizona. We are a relatively small business with approximately 115 employees.

CardSystems has been in operation for over 15 years, and has been processing payment transactions for more than 8 years. We currently handle payment transactions for over 110,000 small to mid-sized businesses, including restaurants, retail shops and local government entities. CardSystems, like other processors, routes

requests for transaction authorization from the point of sale (such as a card swipe terminal) to a payment card network, and then arranges for settlement of funds back to the merchant, although CardSystems does not actually receive or disburse those funds.

In order to gain access to the Visa and MasterCard networks, processors are required to obtain sponsorship from a Visa or MasterCard member bank. As I previously noted, CardSystems' sponsoring bank is Merrick Bank of South Jordan, Utah. Merrick Bank is a member of both Visa and MasterCard, and acts as a liaison between CardSystems and the card associations.

In addition to Visa and MasterCard, CardSystems authorizes transactions for American Express, Discover, JCB and Diners Club.

Data Security Standards in the Payment Card Industry

All merchants and service providers that store, process or transmit cardholder data are directed by the payment card networks to follow security standards. Before December 2004, these standards varied by network. Visa required compliance with its Cardholder

Information Security Program (CISP), which included a mandatory audit by a Visa-certified assessor.

In late Fall 2003, CardSystems was audited and certified by a qualified Visa CISP security assessor, Cable & Wireless. The Cable & Wireless audit, which concluded that CardSystems was unequivocally in compliance with Visa's CISP requirements, was reported to Visa in December 2003. The 2003 CISP audit determined that there were no deficiencies which were not covered by compensating controls. As a result, Visa qualified CardSystems as security-compliant in June 2004. Based on Visa's acceptance, CardSystems relied upon the CISP audit and certification as an assurance that it was compliant.

More recently, the payment card industry has developed a standard known as the Payment Card Industry Data Security Standard (or "PCI" Standard). The PCI Standard is based upon Visa's CISP, and was adopted by Visa, MasterCard, Discover, American Express, Diners and JCB in December 2004 to align their data security programs into a single uniform set of requirements.

The combined PCI Standard lists twelve requirements that all retailers, online merchants, data processors and other entities handling payment card data must meet, such as requiring installation and maintenance of a firewall and anti-virus software and regular virus definition updates. The PCI Standard also sets technology mandates, including requirements for secure storage of data. Entities that do not comply with the mandated security requirements may face sanctions.

Visa and MasterCard required all entities handling payment card data to comply with the PCI Standard by June 30, 2005. In light of CardSystems' recent incident, Visa and MasterCard had agreed to extend the time for CardSystems to conclude its PCI audit until August 31. CardSystems expects to be fully certified as compliant with the PCI Standard requirements at that time. While MasterCard continues to indicate that our compliance will allow us to remain an approved processor, Visa has this week changed its mind, and as of now plans to terminate us no later than October 31, 2005.

How the Security Breach Occurred

In September 2004, an unauthorized party placed a script (a sequence of instructions interpreted or carried out by another program) on the CardSystems platform (an underlying computer system on which application programs run) through an internet-facing application that is used by our customers to access data. In contrast to scripts, viruses and worms are programs or programming code that replicate indiscriminately and may result in file destruction.

This script ran on our system and caused records to be extracted, zipped into a file, and exported to an FTP site (similar to a web address). It was a sophisticated script that targeted a particular file type, and was scheduled to run every four days. Based on all of the forensic investigations conducted externally, by independent scans and investigations and by the payment card providers, we know of only one confirmed instance in which any data was exported, and that is the May 22 incident that has brought us here today.

The offending script searched our computer servers for records with track data (the data on a card's magnetic stripe, which is affixed

to cardbacks and contains identifying data). The most complete information that could have been obtained for any one cardholder would have been that person's name, account number, expiration date and CVV code (contained in the magnetic stripe). Since this data does not include the cardholder's social security number, we believe that there is virtually no risk of identity theft resulting from this intrusion.

The data stored in the files that were confirmed to have been exported by the script consisted of transactions which were not completed for a variety of reasons. This data was stored for research purposes in order to determine why these transactions did not successfully complete. As we have repeatedly acknowledged, our error was that the data was kept in readable form in violation of Visa and MasterCard security standards. As of May 27, 2005, track data is no longer stored by CardSystems.

Number of Consumers Impacted by the CardSystems Security Breach

As the result of the extensive forensic analysis in which we have participated, we know for certain that three files were wrongfully

removed from the CardSystems platform. Of these three files, one was empty, one contained about 4,000 records, and the third contained approximately 259,000 records. The total 263,000 records correspond to 239,000 discrete account numbers. The only records that are confirmed to have left the CardSystems platform were those 263,000 records (representing the 239,000 unique account numbers) that were exported on May 22.

From the card numbers extracted from CardSystems' archived data, the card associations have been able to determine which card issuing banks were affected. By virtue of the rules governing the payment card industry which were enacted in part to protect the privacy of cardholder information, CardSystems does not possess the data that would enable it to notify cardholders who may have been impacted by this incident. Instead, the card issuing banks, through their direct relationship with cardholders, have the complete records that include the names and addresses of cardholders.

So far, out of all of the account numbers that may have been affected, we have not been notified of any that have been used

fraudulently. As I have indicated, the security systems in place in the payment card industry are set up to ensure that minimum cardholder account information is provided to payment processors like us. This also means that CardSystems has no access to the information which would provide us the means to directly monitor consumer fraud. The payment card networks and the card issuing banks, on the other hand, do have such means, and they are continuing to closely monitor cardholders' accounts.

Steps CardSystems is Taking to Prevent Any Future Security Breach

Almost immediately after the breach was detected, CardSystems contacted an outside security solutions firm located in Tucson to identify any additional vulnerabilities from further outside intrusion, and to insure that the actions taken by CardSystems personnel shortly after the intrusion was discovered would prevent the script from continuing to run.

Merrick Bank also retained security assessment and forensic experts immediately after Memorial Day. The role of these experts was to identify the source of the compromise, ensure that there was no

risk for continued compromise, and recover as much data as possible to identify the full extent of the breach.

Merrick's experts determined that the breach resulted in the installation of a script onto CardSystems' computer system through an internet-facing web application in September 2004.

CardSystems continues to cooperate with the inquiries of the regulatory agencies, the FBI, Merrick Bank and the card associations. We continue to focus intensely on remediation and implementation of best practices security as defined by outside security assessment and forensic experts. We have been particularly focused on complying with Visa CISP and PCI standards. For example, CardSystems no longer stores track data, and all track data is now otherwise masked or rendered unreadable.

Based on CardSystems' efforts to address the situation and to ensure that it does not recur, Visa and MasterCard agreed to extend the deadline for CardSystems' PCI security compliance to August 31, 2005. In conjunction with our efforts to achieve PCI security compliance by August 31, we have selected AmbironTrustWave, a

Qualified Data Security Company (QDSC), to perform our official PCI Standard assessment. The assessment will enable us to mitigate risk by validating compliance with the PCI Standard, and therefore with the data security programs of Visa, MasterCard, Discover, American Express, Diners and JCB.

Conclusion

As Chairman Spencer Bachus noted in his opening statement before the Subcommittee on Financial Institutions and Consumer Credit on May 18, 2005, "[e]ven the most prudent company can become the victim of a hacker or other criminal." While we agree with this, CardSystems is learning from this breach and improving the way we do business. CardSystems remains committed to protecting its customers and to ensuring the security of cardholder data.

Madame Chairman, this Subcommittee is to be commended for dedicating its time and attention to the important issues we are discussing today. Thank you for allowing us to participate.

STATEMENT

OF

STEVE RUWE

ON BEHALF OF

VISA U.S.A. INC.

BEFORE THE

SUBCOMMITTEE ON

OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

Credit Card Data Processing: How Secure Is It?

July 21, 2005

Chairwoman Kelly and Members of the Subcommittee, my name is Steve Ruwe. I am the Executive Vice President of Operations and Risk Management 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. 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 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 and, in some cases, the merchants that honor

Visa cards, 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. Typically, these losses are borne by the card issuer; however, 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 a 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. In order to protect its members from these costs, Visa aggressively protects the customer information of its members.

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 the 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 ("AVS") 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 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, only yesterday Visa and the U.S. Chamber of Commerce 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 share responsibility to protect cardholder information.

Security Breach Incident Involving The Payments Processor

Visa was recently informed by payments processor CardSystems Solutions, Inc. ("CSSI") about an unauthorized intrusion into CSSI's computer system. As soon as Visa was aware of this potential breach, Visa immediately began working with the processor, law enforcement and affected member financial institutions to prevent card-related fraud. While the initial investigation was underway, Visa respected standard law enforcement protocol regarding keeping information about the investigation confidential.

After being notified by the processor, Visa's rapid response quickly went to work with our member banks to monitor and manage potentially exposed accounts. Some of our member banks have their own fraud monitoring systems to supplement the Visa monitoring systems.

Visa notified all of the potentially affected card-issuing banks and provided them with the necessary information so that they could monitor the accounts independently, and, if necessary, advise customers to check their statements or cancel and reissue cards to their customers. The card-issuing financial institutions that are members of the Visa system have the direct relationship with their customers who carry Visa cards, and because of Visa's Zero-Liability policy for cardholders, bear most of the financial loss if fraud occurs. These institutions are in the best position to determine the appropriate action with respect to each customer account that might have been affected by a security breach such as the CSSI breach.

To date, we have determined that approximately 22 million Visa card numbers from the CSSI database were put at risk. In many of those cases, CSSI, by its own admission, knowingly and improperly retained magnetic stripe information that can be

used to help create counterfeit cards. This action by CSSI was a clear violation of the CISP. Visa believes that there is no valid reason for merchants or acquirers to retain security code information. Retention of this information in a database makes the database a much more attractive target for criminals and would require more robust security and additional costs. As a result of CSSI's failure to follow Visa security requirements, Visa is terminating CSSI's ability to act as a processor for Visa members.

Significantly, the information that was retained by CSSI did not include the cardholder's date of birth, address, social security number or driver's license number. As a result, Visa believes that the information involved in this incident cannot be used to commit identity fraud against any of the potentially affected individuals in which a criminal opens a new account in the individual's name.

Protecting our cardholders was—and remains—Visa's primary goal throughout the process of responding to this incident. We are actively monitoring the situation on a real-time basis, using our state-of-the-art fraud-fighting technologies, such as Advanced Authorization and Visa's neural networks. Visa will continue to protect for our cardholders and assist law enforcement in their efforts to find those who are responsible for this crime.

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 David B. Watson

Chairman, Merrick Bank

before the House Committee on Financial Services

Subcommittee on Oversight and Investigations

regarding Security of Credit Card Data Processing

July 21, 2005

Madam Chair, Mr. Gutierrez and Members of the Subcommittee:

On behalf of Merrick Bank, thank you for the opportunity to testify before the Subcommittee on the issue of credit card security. As a cardholder and as Chairman of a card-issuing bank, I commend this Committee for its diligence and interest in formulating good public policy on a topic of intimate importance to virtually every American. Merrick Bank is a Utah financial institution, subject to regulation and annual examination by the FDIC and the Utah Department of Financial Institutions. We issue credit cards to account holders, and we make payments of processed credit card transactions to merchants. Both services are important to our customers and to the merchants, and we apply stringent privacy and data integrity standards to both. Credit card and account holder security is a fundamental principle of our business. It has to be.

The specific subject of this hearing is data security. There have been several well-publicized financial data security breaches over the past few months, the most recent involving the credit card transactions processor CardSystems Solutions. Merrick is one of at least seven banks which make payments to merchants who use CardSystems for processing. Although any potential breach of private data raises serious issues, the nature of merchant card processing does limit the

amount of data, which might be exposed by the processor. The merchant processor does not typically have the kind of personal identifying information of the cardholder which would precipitate identity theft; rather it has transaction data, which could be used to perpetrate fraudulent transactions. It is unknown at this point the extent to which the CardSystems breach has resulted in any attempted fraudulent transactions and, like other card issuing banks, we are aggressively monitoring accounts to detect any potential fraudulent transactions.

Today we will describe the card payment process, the specifics of the background and breach by CardSystems, and detail our actions, both regarding CardSystems and with any card processor we use.

Any bank's involvement with credit cards is as a partner with other key players in the transaction chain. Each entity involved in credit cards, including card issuing banks, merchants, card processors, transaction payment banks, and Visa and MasterCard must properly and accurately fulfill its role to assure the protection of the consumer. The integrity and security of the process is strong when the performance by each party is strong.

To most consumers, the credit card system is simple and dependable. But behind the consumer's view of that simple process of charging a purchase, there is a sophisticated series of steps involving several players for each transaction, a series of steps that is repeated millions of times daily.

Most consumers are generally aware of how a credit card is issued. Consumers apply and, after approval, are issued credit cards by financial institutions. This process is reasonably straightforward in terms of data security. In most cases the consumer's billing information is maintained by the issuing institution and used to generate monthly statements and to record payments. The issuing bank must ensure the security of its own credit card program. Merrick Bank is a significant issuer of credit cards. This security issue, however, arose not with the issuing part of the credit card system, but with the merchant transaction processing part. We and other banks make payments to merchants who use CardSystems for processing.

Maintaining and upgrading our card data security systems is a major priority, and must be for any financial institution. Our commitment to the industry standards of security in this field is reflected by our insistence that CardSystems meet the formal Visa accreditation standards before we began our business relationship with them, and our aggressive steps to investigate the problem and assure immediate remediation after we were informed of the data breach by CardSystems on May 25, 2005. We are committed to ensuring that any processors with whom we work are compliant with the industry standards of data security. We want to work with the Committee and other participants in this process toward improvements that would help ensure that systems we work with will protect consumer data. As technology advances, so inevitably does the sophistication of hackers and others who attempt to misuse or breach the technology.

It is useful to describe the broad picture as to how card processing works in general and in our experience. Credit card transaction processing is a multi-party transaction, involving not only card holders, merchants and their processors, but also the card issuing bank, the merchant

payment bank, and the card associations. The merchant either does business directly with the processor or, particularly for smaller merchants, through an independent sales organization (ISO) which aggregates many small merchants and arranges for their processing. The cardholder initiates the transaction with the merchant. The processor performs the "back office" operation of seeing that the transaction is authorized, sending notice for payment to the cardholder's bank, and ensuring that the merchant is paid for the transaction. In some cases processing agents are themselves banks and can make the payments. In many cases the processor or the ISOs have agreements with banks to make the payments of approved charges to merchants. The paying bank is reimbursed by the card issuing bank through the Visa or MasterCard settlement network.

All of these operations are conducted according to rules imposed by the Visa and MasterCard Associations and other card systems. In the case of CardSystems, its transactions predominantly involve Visa and MasterCard acardholders. The Associations reserve the right to approve the issuers of cards and the processors of card transactions. The Association rules dictate standards for card processing. They set forth the procedures which merchants and processors must use for processing various types of transactions, including handling fraudulent transactions.

Aside from this regulation of typical day-to-day transaction activities, Visa and MasterCard have developed, over the past five years, a specific accreditation program for card processors. As of January 1, 2005, Visa, MasterCard, American Express, and Discover have agreed on one set of criteria, Payment Card Industry (PCI) Data Security Standards, to unify the standards and certification processes, which had developed separately over the past few years. PCI approval must be certified by an outside auditor, which itself is certified by Visa, MasterCard and the

other card companies as eligible to make a PCI assessment. After the initial PCI approval, card processors are required to undertake an annual audit, again to be performed by an Association-approved reviewing firm. Should there be disputes about activities of any participants in the card processing system, which include merchants, processors, and paying banks, the Associations reserve the right to determine remedies against various parties.

With that background, I will describe Merrick's perspective on the CardSystems Solutions events.

Merrick has been working with merchants and card processors for more than five years. In September 2003, we were approached by representatives of CardSystems regarding the development of potential business with CardSystems and regarding the transfer of certain ISO contracts to Merrick from Provident Bank. CardSystems was a known entity in the card processing field, having been engaged in card processing with a number of banks for several years. CardSystems was doing business with at least five other banks in addition to Provident Bank. We did not have any significant business contacts with CardSystems before 2003. During a preliminary due diligence review following those 2003 discussions, we determined that CardSystems was not CISP certified by Visa. CISP, the Cardholder Information Security Program, was VISA's data security standard and accreditation process prior to the adoption of today's PCI data security standards. Visa had implemented the CISP standards in 2001, and was allowing processors like CardSystems until September 30, 2004 to secure this CISP certification. We advised CardSystems that we would not consider participating in any processing transactions with CardSystems until and unless CardSystems became CISP certified.

CardSystems engaged an auditor, Cable & Wireless Security, from the Visa-approved auditor list to conduct the CISP assessment. That assessment appears to have begun in 2003, while our predecessor Provident Bank was acting as a merchant payment bank for CardSystems. Cable & Wireless was selected by CardSystems and paid by CardSystems. The audit report was sent by Cable & Wireless to Visa. Cable & Wireless reported to CardSystems and to Visa that CardSystems had taken the necessary steps to be compliant with Visa's CISP standards. In June 2004 Visa informed CardSystems that it deemed CardSystems an approved Association processor, CardSystems so advised Merrick, and we then confirmed with Visa.

The Cable & Wireless "Visa U.S.A. Cardholder Information Security Program (CISP) Service Provider Report on Compliance" (the Report) stated that CardSystems

> has implemented sufficient security solutions and operates in a manner that is consistent with industry best practices and the intent of Visa's CISP program. CardSystems is dedicated to protecting the security of their customer' [sic] information and approaches the process of security with determination.

Further, the Report concluded that

> [t]he results of this assessment will provide CardSystems and VISA U.S.A. with valuable assurance that appropriate precautions have been taken to secure sensitive cardholder data, and will assist in upcoming annual compliance audits.

The Report asserted that the audit included a thorough evaluation of CardSystems' operating environment, including "all systems and network components that retain, store or transmit cardholder data". The Report stated that the Security Engineers completed their review by complying with Visa's standards, performing assessments on the selected systems outlined in the Visa U.S.A. CISP Security Audit Procedures and Reporting and utilizing Visa's *Testing Procedures* as the primary guide to evaluate CardSystems for compliance with the CISP.

With CardSystems having met our requirement to become CISP certified, as determined by the auditor and Visa, we negotiated with Provident Bank and other parties over the assignment of their merchant payment contracts and ISO agreements. These negotiations were successful, and the assignment of payment responsibilities from Provident Bank to Merrick was effective September 30, 2004.

From that point to May 2005, Merrick's payments for the transactions presented by CardSystems proceeded routinely. On May 22, 2005, CardSystems identified a security breach in its operation, and on May 23 contacted the FBI. On May 25, CardSystems contacted Merrick and advised us of a possible intrusion and export of cardholder data at CardSystems. Merrick reviewed this information and notified VISA and MasterCard of the potential security breach. On May 27, 2005, with the approval of VISA and MasterCard, Merrick engaged Ubizen (a well known forensic IT audit firm) to thoroughly investigate the security breach at CardSystems, and Ubizen began an onsite examination of CardSystems at its Tucson facility on May 31, 2005. We also sent our Chief Security Officer and Senior Network Engineer to the CardSystems site to investigate the issue and see that immediate action was taken to prevent any further data breach.

The forensic audit has identified two issues at CardSystems which, in combination, made this breach possible. First, CardSystems retained certain transaction data on their system in clear violation of Association rules. These data retention practices were inconsistent with CISP standards, and it is unclear to us why the Cable and Wireless Report did not note any objection to

the practice, which was ongoing when the CISP certification was approved by Visa in 2004. Ubizen reports this data retention practice had been followed by CardSystems since 1998.

Second, Ubizen identified certain issues with CardSystems servers and software, which were compromised by the intruder. The Cable & Wireless Report did not make any mention of these system vulnerabilities. Ubizen reports that CardSystems servers showed evidence of unauthorized activity as early as April 2004. The Ubizen report does not confirm, however, any actual data export until May 2005. It has been reported that as many as 40 million accounts may have been exposed. That estimate is based on the number of unique accounts authorized by CardSystems from August 2004 to May 2005. The investigation of exactly how much data was actually exported confirms only one export of information on about 263,000 cards. This is a serious and troublesome breach to be sure, and we are committed to dealing aggressively with any breach regardless of the number of cardholders involved.

Merrick, Ubizen, CardSystems, Visa and MasterCard have been aggressively working together to see that the IT issues permitting the breach are corrected and that the CardSystems data environment is firmly secured. Visa and MasterCard have identified the cardholders whose accounts they believe may have been compromised and have sent notice to the issuing banks of the potentially affected cardholders. This was accomplished by June 17, 2005.

Merrick is taking three further steps. First, in consultation with the Associations we have carefully evaluated the findings of the forensic auditor and required CardSystems to immediately address the issues the assessment has raised. Second, Merrick, immediately upon being notified

of the breach, initiated a search for alternate processors to serve our client merchants. Finally, in consultation with security and data experts, Merrick is developing its own set of requirements for card processors for whom we make payments to assure their compliance with all applicable card association standards. For example, not only will processors have to be current with the PCI certification and annual audit requirements, but they must continue to allow Merrick or its auditor to do separate examinations .

I want to conclude by reiterating our absolute commitment to data security in the card transaction and payment process. Merrick insisted upon and relied upon the CISP certification for CardSystems. When we were informed of the breach, we immediately called in expert forensic IT auditors and insisted upon immediate remediation. We are very closely monitoring the accounts of any of our potentially affected cardholders whose for unusual activity. We have been and will continue to work with our processors and Visa and MasterCard to ensure that the processing system continues to function with security, dependability and integrity. I want to again commend this Committee for its hard and good work to formulate sound public policy that will assist in achieving that goal. Thank you.

Statement for the Hearing Record
Submitted By
ARMA International

To the
Committee on Financial Services
U.S. House of Representatives
Washington, DC

Regarding its Hearing on
Credit Card Data Processing: How Secure Is It?

July 21, 2005

About ARMA International

Established in 1956, ARMA International (ARMA) is the non-profit membership organization for the records and information management profession. The 10,000 members of ARMA include records and information managers, imaging specialists, archivists, technologists, legal administrators, librarians, and educators. Our mission includes providing education, research, and networking opportunities to information management professionals, as well as serving as a resource to public policy makers on matters related to the integrity and importance of records and information.

ARMA also serves as a recognized standards developer for the American National Standards Institute (ANSI), participating and contributing toward the development of standards for records and information management.[1] ARMA is also a charter member of the information and documentation subcommittee of the International Organization for Standardization (ISO), aiding in the development of its records management standard.[2]

Because of the essential role of effective and appropriate information management in today's economy, ARMA International has a strong interest in issues pertaining to safeguarding consumer information and other personally identifiable information possessed by business and government.

Records and information management plays an important role in the private sector. In this new century, the most valuable commodity of business is information, often in the form of data bases of essential information required by the service sectors of our economy. This includes personally identifiable information and other sensitive information of consumers.

The greatest responsibility for organizations will be managing and maintaining the integrity of an ever-growing flow of information, including the establishment of appropriate safeguards for sensitive information and in establishing retention schedules complaint with regulatory and statutory requirements. Issues such as what information has intrinsic value and what information will be shared and with whom are critical to the future success of 21st century organizations. These challenges call for increased recognition of the role of managing critical information and providing appropriate protections for personally identifiable information. ARMA believes that technology alone will not provide the level of

---

[1] The ARMA/ANSI publications are: (1) "Glossary of Records and Information Management Terms" (ANSI/ARMA 10-1999, 2nd ed); (2) "Establishing Alphabetic, Numeric and Subject Filing Systems" (ANSI/ARMA 12-2005); (3) "Framework for the Integration of Electronic Document Management Systems and Electronic Records Management Systems Technical Reports" (ANSI/AIIM ARMA TR48-2004); (4) "Records Center Operations, 2nd ed." (ANSI/ARMA TR-01-2002); (5) "Retention Management for Records and Information" (ANSI/ARMA 8-2005); (6) "Requirements for Managing Electronic Messages as Records" (ANSI/ARMA 9-2004); and (7) "Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records" (ANSI/ARMA 5-2003). See also "Managing Recorded Information Assets and Resources: Retention and Disposition Program" which may be viewed at http://www.arma.org/standards/public/document_review.cfm?DocID=22.

[2] The ISO Standard on "Information and documentation – records management" is published in two parts. ISO 15489-1:2001, "Information and documentation – records management – Part 1: General", contains the International Standard, and ISO/TR 15489-2:2001, "Information and documentation – records management – Part 2: Guidelines", contains the Technical Report.

safeguards against unauthorized access to these data bases; instead, safeguards must include a records and information management program that tasks the human capital of an organization to ensure that records and information are properly maintained, accessed, and ultimately disposed of in accordance to statutory and regulatory requirements as well as consumer expectations.

ARMA firmly believes that organizations that embrace records and information management will add a level of safeguards and accountability not achievable by technology alone. ARMA also believes that organizations that embrace records and information management as being strategic and mission critical will ensure their competitive advantage and remain appropriate stewards of information that contains personal and private records. Any records and information management requirements established by statute or regulation should complement the competitive advantage that records and information management has traditionally promised.

Data Security Initiatives Need to Be Sensitive to a Wide Variety of Factors

Americans demand security and privacy of their personally identifiable information. Identity theft complaints continue to rise.[3] The establishment of new systems that allow easy access and transference of personally identifiable data between parties should to be sensitive to personal privacy and grant assurance to Americans that their data will not be misused or end up in the wrong hands. ARMA believes that these systems must incorporate the best practices of records and information management.

Of primary importance from a records and information management perspective is ensuring the privacy and security of the information. Whatever information management systems are in place must ensure protection of the records and information in these two critical areas. Public sector agencies and private sector entities should not have access to personally identifiable information unless the information is essential to the organization's mission or business mandate. It is important that public and private sector entities identify what information is actually mission critical, who within their organizations should have access to the information, and then ensuring that the information cannot be accessed by unauthorized parties.

Established records and information management policies that follow best practices concerning retention, disposition, categorization, maintenance, or disposal may apply to

[3] The Federal Trade Commission reported over 400,000 complaints of identity theft logged into its ID Theft Clearinghouse as of December 2003. See prepared statement of the Federal Trade Commission on Identity Theft: Prevention and Victim Assistance, presented by Betsy Broder, Assistant Director, Division of Planning and Information, Bureau of Consumer Protection, before the Subcommittee on Oversight and Investigations of the House Committee on Energy and Commerce (December 15, 2003). http://www.ftc.gov/os/2003/12/031215idtheftestimony.pdf. Concerns have also begun to emerge with health care providers, financial institutions, and other users of consumer information sending personally identifiable information overseas for processing. This practice, known as "information offshoring" is becoming more and more common as organizations seek to curb costs by sending data to countries such as India, Pakistan, and Bangladesh for processing. Unfortunately, these nations lack any statutory controls for the protection personally identifiable information and it remains unclear whether existing U.S. laws, such as HIPAA, apply.

aggregated data just as they apply to records in other formats.[4] The requirements for protecting records during their use cannot simply be "added on" at the end of a technology implementation. Records and information management policies are integral to the functioning of any regime which stores, retrieves and protects information, and therefore must be considered during each phase from design to final implementation and system maintenance.

Why Records Retention and Destruction Policies are Important for Data Security

Information is among the most valuable commodities of any organization. In the case of organizations that possess, process, and use sensitive consumer information, this information is a part of the organization's strategic business model. As such, these organizations have a significant responsibility to manage and maintain the integrity and security of this information, including the implementation of appropriate safeguards against unauthorized use and the proper disposal of the information.

ARMA notes that a significant risk of identity theft occurs at a point when a given record should be destroyed – and the best practices of records and information management and a record's retention schedule would require not only appropriate measures to ensure destruction, but also the documentation of the destruction or final disposition action.

Within the context of managing the life cycle of any information, assuring that records and information are destroyed appropriately – at the time and in the manner anticipated by the organization's retention and disposition program, and in compliance with any applicable law or regulation – is as important and deserves the same level of attention and stewardship as assuring that the information is properly maintained – both for the use of an organization in pursuit of its business purposes as well as for safeguarding the information from improper use during the useful life of the information. The appropriate destruction of a record at the end of its life cycle will assist with efforts to curb identity theft, such as the growing problem of "dumpster diving." The same best practices will safeguard the misappropriation of records stored in electronic format.

ARMA's comments are informed by recognized practices of documenting the disposal of information and records. ISO 15489-1 Clause 9.9, "Implementing disposition" provides in part: "The following principles should govern the physical destruction of records –

1) Destruction should always be authorized.
2) Records pertaining to pending or actual litigation or investigation should not be destroyed.
3) Records destruction should be carried out in a way that preserves the confidentiality of any information they contain.
4) All copies of records that are authorized for destruction, including security copies, preservation copies and backup copies, should be destroyed."

[4] See "Managing Electronic Messages as Records (formerly: Guideline for Managing E-mail)" (ANSI/ARMA-9-200x).

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act), approved by this Committee, contains a provision requiring the Federal Trade Commission and the various banking regulators to develop a disposal rule for sensitive customer information. This rule may provide a model for businesses in other industry sectors for the appropriate disposal of personally identifiable information. In its comments to the disposal rules proposed by the Commission and the various banking regulators, ARMA strongly recommended that an orgnization's safeguards include a formal, written records and information management program, consistent with ISO 15489.

Safeguards and proper disposal are essential elements of an organization's information retention and disposition program. ARMA believes that any safeguard regime for personally identifiable information must include the formal endorsement by senior management of a written records and information management program. This would include the appropriate investment in personnel, training and organization-wide communications. It would also ensure that third party relationships endorse the same safeguards with appropriate means of ensuring compliance. This employment of the human capital of an organization will be essential to any safeguard regime. ARMA firmly believes that technology alone does not represent the foundation of an effective safeguard regime.

ARMA recommends specific identification of records and information management in any statutory or regulatory requirement for the establishment of safeguards for sensitive or personally identifiable information. In this regards, the term "records and information management program" means a written statement of policy and procedures put in place to manage the life cycle of information that is endorsed by the chief executive officer of a covered entity, communicated to all employees of the information broker and affiliates or third parties with access to or with responsibilities of the management of covered information, and is based on the best practices of records and information management as informed by the standards developed by the American National Standards Institute with ARMA International or the ISO standard 15489: Information and documentation – Records management, promulgated by the International Organization for Standardization.

In today's distributed work environments, a wide variety of individuals create records and must therefore take responsibility to ensure those records are captured, identified and preserved. It is no longer enough to train administrative staff and assume they will make sure the records end up in the records management program. All members of management, employees, contractors, volunteers and other individuals share the responsibility for capturing records so they can be properly managed throughout the length of their required retention period.

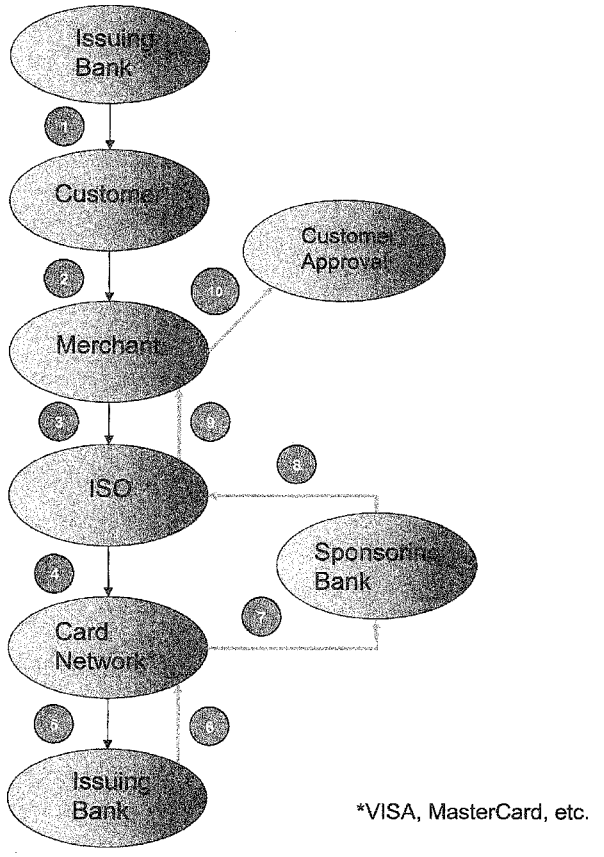
Conclusion

ARMA International applauds the leadership of Chairman Oxley and Ranking Member Frank for examining the data security issue. ARMA recommends to the Committee the best practices of records and information management as an effective element for any data security or safeguards initiatives or policies.

Respectfully submitted,

Cheryl L. Pederson, CRM
President
ARMA International
13725 W. 109th St., Suite 101
Lenexa, KS 66215
800.422.2762/913.341.3808
Fax 913.341.3742

Cardholder Transaction Process



The above chart is a simplified representation of the typical processes a transaction flow might involve and the possible participants. Actual transactions may vary dependent on card type, ISO/Merchant/Bank contract terms, origination source and type of transaction.

Cardholder Transaction Process

ENTITY	TRANSACTION
Issuing Bank	1 Issuing Bank grants credit and issues card to Customer.
Customer	2 Card may be presented in person, by Internet, phone or other remote means.
Merchant	3 Merchant sends card and purchase data to Independent Servicing Organization (ISO). Merchant must have a tri-party agreement with ISO and the Sponsoring Bank to access the Card Network.
ISO	4 ISO sends transaction to Credit Card Network for approval.
Credit Card Network (VISA, MasterCard, etc.)	5 Credit Card Network approves/declines the transaction, and notifies the Issuing Bank. Or the Credit Card Network forwards the transaction to the Issuing Bank for authorization.
Issuing Bank	6 Issuing Bank approves/declines the transaction, and notifies the Card Network. Issuing Bank retains transaction information to send to customer in the account statement.

The above chart is a simplified representation of the typical processes a transaction flow might involve and the possible participants. Actual transactions may vary dependent on card type, ISO/Merchant/Bank contract terms, origination source and type of transaction.

Cardholder Transaction Process

ENTITY	TRANSACTION
Credit Card Network	7 Once the transaction is authorized, the Credit Card Network sends the transaction to the Sponsoring Bank.
Sponsoring Bank	8 Sponsoring Bank receives the transaction. If it has a Merchant reserve account for the Merchant initiating the transaction, Sponsoring Bank adjusts the reserve account. Then, it transmits the transaction to the ISO.
ISO	9 ISO notifies the Merchant whether or not the transaction was approved. ISO retains the information for settlement with the bank during periodic batch process.
Merchant	10 Merchant then delivers the goods or services to the customer. Process takes up to 10 seconds.

The above chart is a simplified representation of the typical processes a transaction flow might involve and the possible participants. Actual transactions may vary dependent on card type, ISO/Merchant/Bank contract terms, origination source and type of transaction.

Page 1: [14] Deleted **jdorsey** **7/8/2005 12:13:00 PM**
Rules

Page 1: [14] Deleted **jdorsey** **7/8/2005 12:16:00 PM**

Page 1: [14] Deleted **jdorsey** **7/8/2005 12:16:00 PM**

Page 1: [15] Deleted **jdorsey** **7/8/2005 1:22:00 PM**
(CardSystems Solutions, Inc.)

Page 1: [16] Deleted **NJohns** **7/11/2005 9:28:00 AM**

Sponsoring Banks	Regulatory AgencyFederal Banking Laws, Rules and Regulations; Visa/MC Rules; FTC Act	Primary Bank Regulator; VVisa/MC via Membership agreements	Informal and formal actions, fines. Termination	Unlimited	Charge

Page 1: [17] Deleted **jdorsey** **7/8/2005 1:22:00 PM**
Visa/MasterCard Organization

Page 1: [18] Deleted **NJohns** **7/11/2005 10:00:00 AM**
[Bank Service Company Act]

Page 1: [19] Deleted **NJohns** **7/11/2005 9:27:00 AM**

Issuing Banks	Federal Banking Regulatory Laws, Rules and Regulations; Visa/MC Rules; FTC Act	Primary Bank Regulator; VVisa/MC via Membership agreements	Informal and formal actions, fines. Termination	Unlimited	All cust informa

Page 1: [20] Change **jdorsey** **7/8/2005 12:11:00 PM**
Formatted Table

Page 1: [21] Deleted **jdorsey** **7/8/2005 12:08:00 PM**
Each of the v

Page 1: [21] Deleted **jdorsey** **7/8/2005 12:08:00 PM**
States

Page 1: [1] Formatted jdorsey 7/8/2005 1:30:00 PM
Top: 72 pt, Bottom: 72 pt

Page 1: [2] Deleted FDIC 7/8/2005 4:49:00 PM

Credit Card Transaction Participants Table

Page 1: [3] Formatted jdorsey 7/8/2005 1:22:00 PM
Centered

Page 1: [4] Change jdorsey 7/8/2005 1:22:00 PM
Formatted Table

Page 1: [5] Deleted jdorsey 7/8/2005 12:11:00 PM

Page 1: [5] Deleted jdorsey 7/8/2005 12:11:00 PM

Page 1: [6] Deleted mpetermann 7/11/2005 8:10:00 AM
. Also may ask for driver's license, address, telephone number

Page 1: [7] Deleted jdorsey 7/8/2005 12:11:00 PM

Page 1: [7] Deleted jdorsey 7/8/2005 12:20:00 PM
Rules

Page 1: [7] Deleted jdorsey 7/8/2005 12:14:00 PM
under
Sponsoring agreements

Page 1: [8] Deleted jdorsey 7/8/2005 1:21:00 PM
Acquiring

Page 1: [8] Deleted jdorsey 7/8/2005 12:09:00 PM
Rules

Page 1: [9] Deleted FDIC 7/8/2005 4:49:00 PM

Merchant Banks	Federal Banking Regulatory Laws, Rules and Regulations; Visa/MC Rules; FTC Act	Primary Bank Regulator; Visa/MC Rules undervia Membership agreements	Informal and formal actions, fines. Termination	Unlimited (1)	Cardhol

Page 1: [10] Change jdorsey 7/8/2005 12:11:00 PM
Formatted Table

Page 1: [11] Deleted jdorsey 7/8/2005 12:11:00 PM

Page 1: [11] Deleted jdorsey 7/8/2005 12:11:00 PM

Page 1: [12] Deleted jdorsey 7/8/2005 12:13:00 PM
GLBA contractual requirements from banks

Page 1: [13] Deleted jdorsey 7/8/2005 12:11:00 PM

Page 1: [13] Deleted jdorsey 7/8/2005 12:17:00 PM
Rules under Sponsoring agreements and membership agreements

Page 1: [14] Deleted jdorsey 7/8/2005 12:16:00 PM

Regulatory Oversight Table

Participant	Applicable Regulations & Requirements (1)	Enforcing Entity (1)	Enforcement Available	Customer Data Holding Period	Type Of Customer Data Held
Issuing Banks	Federal Banking Laws, Rules and Regulations; Visa/MC Rules; FTC Act	Primary Bank Regulator; Visa/MC via Membership agreement	Informal and formal actions, fines, Termination	Unlimited	All customer credit card and credit history information from credit reports
Merchants (includes Internet, telephone, point of sale, and in person transactions)	FTC Act; FTC Safeguard Rules; Visa/MC Rules; Sponsoring Bank contract	FTC; Visa/MC or Sponsoring Bank	Fines, termination of agreements	One processing day for expiration and verification code	Cardholder name, number, expiration date, and verification code
				Unlimited	Also may ask for driver's license, address, telephone number
Independent Service Organization (ISO)	FTC Safeguard Rules; Visa/MC Rules; Sponsoring Bank contract (incorporating GLBA reqmts); Bank Service Company Act; FTC Act	Primary Bank Regulator/FTC; Visa/MC or Sponsoring Bank	Informal and formal actions, fines, Termination of Contracts and Agreements	One processing day	Card verification code and expiration date
				Unlimited	Cardholder name and number
Card Networks	Bank Regulatory Agency GLBA Rules; FTC Act; FTC Safeguard Rules; Federal Banking Laws	Bank Regulatory Agencies/FTC	Informal and formal actions, fines	Unlimited	Access to all Visa/MC credit card information
Sponsoring Banks	Federal Banking Laws, Rules and Regulations; Visa/MC Rules; FTC Act	Primary Bank Regulator; Visa/MC via Membership agreement	Informal and formal actions, fines, Termination	Unlimited	Obtains bank cardholder, name and number

(1) Various States may have laws that may impact each of these participants, for instance the California customer notification law.

Note: This chart represents a simplified, general description of the participants in credit card transactions. It highlights only the major pertinent laws, regulations and agreements, and is not intended to be comprehensive. The participants, applicable laws, and government agencies and other entities with authority may vary depending on the facts of a particular case.

Formatted ... [1]
Deleted: Credit Card Transactio ... [2]
Deleted: Enforcement
Formatted ... [3]
Formatted Table ... [4]
Deleted: s
Deleted: Action
Deleted: (2)
Deleted: ¶ ... [5]
Deleted: ¶
Deleted: ¶
Deleted: . Also may ask for d ... [6]
Deleted: ¶ ... [7]
Deleted: Acquiring…Rules ... [8]
Deleted: ¶ ... [9]
Formatted Table ... [10]
Deleted: ¶ ... [11]
Deleted: ¶
Deleted: GLBA contractual r ... [12]
Deleted: ¶
Deleted: ¶ ... [13]
Deleted: ¶
Deleted: ¶
Deleted: ¶ ... [14]
Deleted: (CardSystems Sol ... [15]
Deleted: ¶ ... [16]
Deleted: ¶
Deleted: Visa/MasterCard¶ ... [17]
Deleted: ¶
Deleted: Bank Service Com ... [18]
Deleted: ¶ ... [19]
Formatted Table ... [20]
Deleted: Each of the v…States ... [21]