AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# FIGHTING FRAUD: IMPROVING INFORMATION SECURITY

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

AND THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

APRIL 3, 2003

Printed for the use of the Committee on Financial Services

**Serial No. 108–19**

U.S. GOVERNMENT PRINTING OFFICE

89–407 PDF WASHINGTON : 2003

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
DOUG BEREUTER, Nebraska
RICHARD H. BAKER, Louisiana
SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
ROBERT W. NEY, Ohio
SUE W. KELLY, New York, *Vice Chairman*
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LATOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, JR., North Carolina
DOUG OSE, California
JUDY BIGGERT, Illinois
MARK GREEN, Wisconsin
PATRICK J. TOOMEY, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN B. SHADEGG, Arizona
VITO FOSELLA, New York
GARY G. MILLER, California
MELISSA A. HART, Pennsylvania
SHELLEY MOORE CAPITO, West Virginia
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
TIM MURPHY, Pennsylvania
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
KATHERINE HARRIS, Florida
RICK RENZI, Arizona

BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELÁZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
BARBARA LEE, California
JAY INSLEE, Washington
DENNIS MOORE, Kansas
CHARLES A. GONZALEZ, Texas
MICHAEL E. CAPUANO, Massachusetts
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
KEN LUCAS, Kentucky
JOSEPH CROWLEY, New York
WM. LACY CLAY, Missouri
STEVE ISRAEL, New York
MIKE ROSS, Arkansas
CAROLYN MCCARTHY, New York
JOE BACA, California
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
RAHM EMANUEL, Illinois
DAVID SCOTT, Georgia
ARTUR DAVIS, Alabama

BERNARD SANDERS, Vermont

Robert U. Foster, III, Staff Director

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

SPENCER BACHUS, Alabama, *Chairman*

STEVEN C. LATOURETTE, Ohio, *Vice Chairman*
DOUG BEREUTER, Nebraska
RICHARD H. BAKER, Louisiana
MICHAEL N. CASTLE, Delaware
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SUE W. KELLY, New York
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
WALTER B. JONES, Jr., North Carolina
JUDY BIGGERT, Illinois
PATRICK J. TOOMEY, Pennsylvania
VITO FOSSELLA, New York
MELISSA A. HART, Pennsylvania
SHELLEY MOORE CAPITO, West Virginia
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
TIM MURPHY, Pennsylvania
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
RICK RENZI, Arizona

BERNARD SANDERS, Vermont
CAROLYN B. MALONEY, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
LUIS V. GUTIERREZ, Illinois
DENNIS MOORE, Kansas
CHARLES A. GONZALEZ, Texas
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
NYDIA M. VELÁZQUEZ, New York
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
KEN LUCAS, Kentucky
JOSEPH CROWLEY, New York
STEVE ISRAEL, New York
MIKE ROSS, Arkansas
CAROLYN MCCARTHY, New York
ARTUR DAVIS, Alabama

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

SUE W. KELLY, New York, *Chair*

RON PAUL, Texas, *Vice Chairman*
STEVEN C. LATOURETTE, Ohio
MARK GREEN, Wisconsin
JOHN B. SHADEGG, Arizona
VITO FOSSELLA, New York
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
TIM MURPHY, Pennsylvania
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina

LUIS V. GUTIERREZ, Illinois
JAY INSLEE, Washington
DENNIS MOORE, Kansas
JOSEPH CROWLEY, New York
CAROLYN B. MALONEY, New York
CHARLES A. GONZALEZ, Texas
RUBEN HINOJOSA, Texas
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts

# CONTENTS


| | Page |
|---|---|
| Hearing held on: | |
| April 3, 2003 | 1 |
| Appendix: | |
| April 3, 2003 | 53 |


## WITNESSES

### THURSDAY, APRIL 3, 2003


| | |
|---|---|
| Beales, J. Howard III, Director, Bureau of Consumer Protection, Federal Trade Commission | 11 |
| Brady, John J., Vice President, Merchant Fraud Control, MasterCard International | 33 |
| Caddigan, Tim, Special Agent in Charge, Financial Crimes Division, United States Secret Service, accompanied by Robert Weaver, Deputy Special Agent in Charge, New York Field Office | 8 |
| Farnan, James E., Deputy Assistant Director, Cyber Division, FBI | 10 |
| Hendricks, Evan, Editor and Publisher, *"Privacy Times"* | 34 |
| McIntyre, David J. Jr., President and CEO, TriWest Healthcare Alliance | 25 |
| Mitnick, Kevin D., President and Co-founder, Defensive Thinking | 27 |
| Pratt, Stuart, President, Consumer Data Industry Association | 31 |


## APPENDIX


| | |
|---|---|
| Prepared statements: | |
| Bachus, Hon. Spencer | 54 |
| Kelly, Hon. Sue W. | 56 |
| Oxley, Hon. Michael G. | 58 |
| Gillmor, Hon. Paul E. | 60 |
| Hinojosa, Hon. Rubén | 61 |
| Paul, Hon. Ron | 63 |
| Shadegg, Hon. John B. | 65 |
| Beales, Howard | 67 |
| Brady, John J. | 86 |
| Caddigan, Timothy | 92 |
| Farnan, James E. | 98 |
| Hendricks, Evan | 105 |
| McIntyre, David J. Jr. | 114 |
| Mitnick, Kevin | 124 |
| Pratt, Stuart K. (with attachments) | 130 |
| Weaver, Bob | 141 |


## ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD


| | |
|---|---|
| Assistant Secretary of Defense, William Winkenwerder, Jr., prepared statement | 145 |
| Farnan, James E.: | |
| Written response to questions from Hon. Sue W. Kelly | 150 |
| Hendricks, Evan: | |
| Written response to questions from Hon. Sue W. Kelly | 151 |

Page

McIntyre, David J. Jr.:
Written response to questions from Hon. Sue W. Kelly ..... 153
Mitnick, Kevin:
Written response to questions from Hon. Sue W. Kelly ..... 156

# FIGHTING FRAUD: IMPROVING INFORMATION SECURITY

**Thursday, April 3, 2003**

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
JOINT WITH THE SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
*Washington, D.C.*

The subcommittee met, pursuant to call, at 10:07 a.m., in Room 2128, Rayburn House Office Building, Hon. Sue W. Kelly [chairwoman of the Subcommittee on Oversight and Investigations] presiding.

Present: Representatives Bachus, Kelly, Shadegg, Fossella, Capito, Tiberi, Feeney, Hensarling, Murphy, Barrett, Renzi, Maloney, Gutierrez, Hooley, Carson, Sherman, Inslee, Moore, Ford, Lucas of Kentucky, McCarthy, and Matheson.

Chairwoman KELLY. The Committee on Oversight is pleased to be able to have this hearing today.

Personal information has to be safeguarded throughout our national credit system. Just as consumers shred their unwanted mail and take care with their receipts, financial institutions have to develop and upgrade their information security procedures to protect consumers. Financial records such as credit card numbers are combined with other pieces of personal information, and they are the first targets of identity thieves. Years of work are often necessary for both consumer and business victims to correct damaged credit histories and restore access to credit.

Today two subcommittees will hear from the witnesses on three specific case studies to review current industry practices and to ensure that proper security procedures and protocols are in place or are being implemented.

Teledata Communications is a company in my home State of New York that enables businesses to access credit bureau information so they can grant credit to consumers. An employee inside the company allegedly stole and sold passwords and codes for accessing credit reports for thousands of people. According to law enforcement, his actions resulted in millions of dollars of financial theft.

TriWest Healthcare, an important health care provider for our active duty military personnel, honored veterans and their dependents, suffered the physical theft of its computer hardware. The equipment stored personal information about many of our heroes now involved in the war to liberate Iraq, including the Chairman

of the Joint Chiefs of Staff, General Richard Myers. Fortunately, quick action by the company and the credit bureaus appears thus far to have prevented misuse of the information.

Another company, Data Processing International, in Nebraska saw its database of millions of credit card numbers hacked from the outside. It again appears that rapid action this time by the company and the credit card companies have prevented improper use of the numbers to date.

Through the examination of these cases the subcommittee will review how credit issuers, third party vendors that process transaction, credit bureaus and law enforcement agencies coordinate efforts to limit harm to consumers when data security is breached. Among our witnesses are officials of the law enforcement and regulatory agencies involved with these and other such cases, representatives of the companies involved, one of the most notorious computer hackers in the world, who is now a consultant, I am happy to report, and an expert in privacy.

I want to thank my distinguished colleague, Representative Spencer Bachus, the chairman of the Subcommittee on Financial Institutions and Consumer Credit, for joining us in holding this important hearing of our subcommittees. I also want to congratulate him for his leadership in the bipartisan passage of H.R. 522, the Federal Deposit Insurance Reform Act of 2003, by the full House yesterday.

With that, I turn to Mr. Gutierrez.

[The prepared statement of Hon. Sue W. Kelly can be found on page 56 in the appendix.]

Mr. GUTIERREZ. Good morning, Chairs Kelly and Bachus, and members of the committee. Today more than ever identity theft takes myriad forms. Modern thieves are using massive digitized databases to access and steal consumers' personal information. As too many people are learning the hard way, identity thieves steal Social Security, bank account, and credit card numbers and use them to commit fraud, very often destroying the credit rating and financial future of their victims. Every year thousands of these victims are left financially ruined, often with severe credit problems and even false criminal records that they must spend years working to erase. Even in minor cases victims spend endless hours.

So we are gathered here today to discuss ways to help consumers by increasing the security of data that contains our personal information and to understand some of the possible loopholes that have enabled these cases to occur in the first place, to hear about data security efforts undertaken by the companies that hold our private information, and look for ways to help consumers have quick and better access to their personal records when identity theft incidents occur. One of the most fundamental problems is consumers are often left out of the loop after their information has been stolen and this is unacceptable.

In one of the cases that will be discussed today a former employee of Teledata is being charged with the biggest identity theft fraud in U.S. history. One of the most outrageous aspects of this specific case is that in March of 2000 the alleged perpetrator quit his job, but that didn't even slow down his scheme. He only worked there for 10 months but the scam continued for 3 years. The com-

pany security codes he allegedly stolen still worked and were accessible right up to the moment of his arrest. In the meantime 30,000 people had their identities stolen and financial losses reached more than $2.7 million.

How could personal data be so easily accessible? What kinds of safeguards do companies have in place to deter these practices? I hope that this hearing will serve as an opportunity to answer these questions and others. I thank you for holding the hearing, and I look forward to the testimony, and I ask unanimous consent that my complete opening statement be submitted for the records.

Chairwoman KELLY. Thank you very much, Mr. Gutierrez. Mr. Bachus.

Mr. BACHUS. Thank you, Chairman Kelly, for telling me my mike wasn't on, that is very important, and also for convening this joint hearing of our two subcommittees to review issues relating to the security of personal information. This is an issue of critical importance to the financial service industry and I believe this hearing is a timely one, and it is actually one of a series of hearings that Chairwoman Kelly has been holding over the past year or two on this issue.

This hearing, which is titled "Fighting Fraud: Improving Information Security," is one of many hearings that will be held by the Subcommittee on Financial Institutions and Consumer Credit regarding the security of personal information. I expect that at some point our efforts will culminate in comprehensive legislation addressing the broad issue of how secure consumers feel with respect to their personal information.

Today's hearing will focus on three cases where sensitive personal information was compromised through hacking or physical theft of computer databases. Each case that we will hear about today is illustrative of a different type of security breach: An outside computer hacker, employee misconduct, and a garden variety burglary. Using these cases, we will review how credit issuers, third party vendors that process transactions, credit bureaus, and law enforcement coordinate efforts to limit harm to consumers when data security is breached.

Fighting fraud and protecting the security of personal information is a topic that unites financial institutions and consumers. Each group is harmed by the fraudulent use of personal information. Financial institutions are the victims of fraud because the financial institution is usually liable for any losses suffered as a result of that fraud. Consumers obviously suffer unnecessary inconvenience and insecurity as a result of fraud and they can be exposed to additional crimes such as identify theft. Furthermore, at least a portion of financial institutions' fraud losses can be expected to be passed on to consumers in the form of higher prices. There can be no doubt that when fraud is committed everyone loses.

For obvious reasons financial institutions take precautions to prevent fraud, including precautions to protect the security of personal information. In addition to the self-interest financial institutions have in minimizing their fraud losses, Congress has required financial institutions to maintain appropriate standards relating to information security, including standards to protect against unauthorized access to a financial institution's customer records as part

of the Gramm-Leach-Bliley Act. The requirements as adopted by the Federal banking agencies also require financial institutions to oversee their relationship with third party service providers, including having the service providers agree by contract to implement a comparable information security program. It is my understanding that the Federal banking agencies have been examining financial institutions with respect to their compliance with these requirements.

However, I remain interested in learning more about the role service providers play with respect to information practices and the ability to maintain appropriate information security programs. It is my understanding that the Bank Service Company Act gives the bank regulators broad authority to examine third party providers. Two of the cases today illustrate that greater oversight of these entities may be necessary.

As part of Gramm-Leach-Bliley, Congress also enacted stiff prohibitions against a practice known as pretext calling, which is a fraudulent means of obtaining an individual's personal information. Pretext callers contact a financial institution's employees and attempt to obtain customer information usually while posing as a customer whose information they are trying to collect. This is a serious issue and one that both Subcommittees—actually the Oversight Committee has held several hearings previously. I am interested in learning more about efforts to enforce this prohibition and the Federal Trade Commission's advice on the amount of resources devoted to fighting this fraudulent practice.

We will also hear this morning from Federal law enforcement agencies about their approach to countering those who would compromise the security of personal information. It has always been my experience that law enforcement and the financial services industry works well together with respect to pursuing those who attempt to commit crimes against consumers and financial institutions. I look forward to hearing about law enforcement's perspective on this important topic, especially with respect to representatives from the FBI, Secret Service and FTC.

In short, financial institutions, Congress, the banking agencies, and law enforcement have been working to address information security and fraud prevention issues. Regardless of the great pains taken by all these parties to protect the security of personal information, the chance remains that a breach may occur. Therefore, Congress must remain vigilant to ensure that existing regulations are implemented appropriately and examine whether new safeguards are necessary. Furthermore, it is just as important for financial institutions to have mitigation plans in place in the event that their information security program is hacked or otherwise compromised.

In conclusion, let me say I am pleased that we will hear from several witnesses today who will describe how various parties took action to address recent breaches and prevent subsequent fraud. Before we proceed I believe it is important to mention to the entire panel that although this hearing is a public forum, we should avoid discussing specific details which may give criminals ideas or even a road map for doing further harm.

Let me close by thanking Chairman Oxley for recognizing the importance of improving the security of personal information and scheduling this hearing. We must continue to work to improve security and protect sensitive data to ensure the consumers continue to have confidence in our nationwide credit system as well as our financial services system in general. I look forward to working with the chairman, Mrs. Kelly, and other colleagues as we continue to examine this complicated issue.

[The prepared statement of Hon. Spencer Bachus can be found on page 54 in the appendix.]

Chairwoman KELLY. Thank you. Mrs. McCarthy, do you have an opening statement?

Mrs. MCCARTHY. Thank you. I will wait for the testimony.

Chairwoman KELLY. Mr. Moore.

Mr. MOORE. Thank you, Madam chair and Congressman Bachus. I appreciate both of you convening this hearing. I appreciate the witnesses being present. I want to reiterate, I won't say it all, what Congressman Bachus and Congresswoman Kelly said before, and that is this is a very important area. As a district attorney for 12 years I worked closely with people in fraud cases and a lot of the things—this was back in the 1970s and 1980s, so a lot of the things we are talking about here today weren't relevant then, weren't even around then. As the Internet has expanded and accessibility of the Internet is used not only by individuals but by financial institutions and other organizations and private and important individual data is contained in databases, I think it is very, very important that we protect that information. I think individuals who have private important information stored in those databases have a right to expect that companies and institutions will take adequate measures to protect that information. Obviously, theft of that information, identity theft and theft of financial information about an individual can cause great harm to a person and to their family, and it ends up costing all the consumers I think a lot of extra money.

So I am interested to hear what the witnesses have to say and very much appreciate you being here.

Thank you.

Chairwoman KELLY. Thank you very much.

Mr. Shadegg.

Mr. SHADEGG. Thank you, Chairwoman Kelly. I want to begin by thanking you and Chairman Bachus for holding this important hearing on information security. I also want to begin by thanking one of my constituents, David McIntyre, president and CEO of TriWest Healthcare Alliance, for agreeing to be here and testify today.

My personal interest in identity theft and information security began about 5 years ago when two of my constituents, Bob and Joanne Hartle of Phoenix, Arizona were victims of identity theft. My constituents, following their victimization, were instrumental in securing the passage of the first State law in the Nation criminalizing identity theft. Mr. and Mrs. Hartle suffered the devastation of identity theft when a convicted felon took Mr. Hartle's identity and made purchases totaling over $100,000. In addition, this individual purchased handguns using Mr. Hartle's clean record to get

around the Brady law. Finally and shockingly in this day of terrorism, this individual also used Mr. Hartle's clean record and military record to obtain security clearance to secure areas of Phoenix Sky Harbor International Airport. As a result of this victimization at a time when there were no State laws and no Federal laws penalizing identity theft, Mr. and Mrs. Hartle were forced to spend more than 4 years of their life and more than $15,000 of their own money seeking to restore their credit.

Their case led me to introduce legislation to criminalize identity theft at the Federal level. The Identity Theft and Assumption Deterrence Act of 1998 was signed into law by President Clinton on October 30th, 1998. It gives for the first time Federal law enforcement agencies, including those who are represented before us here today, the authority to investigate and prosecute identity theft.

But following the passage of that law, I found there was more that needed to be done. We began to notice that the Federal agencies with this new authority were unfamiliar with it and did not have a habit of coordinating with local law enforcement on these issues. So we began a series of meetings that lasted over a year in Phoenix, Arizona between Federal law enforcement agencies, including the FBI and others here today and State and local law enforcement agencies, to try to resolve the tough issues of who should act and what they should do in the interplay between Federal and State laws and in the interplay of these crimes where someone is victimized in one place but lives many States away, thousands of miles away.

Mr. and Mrs. Hartle also turned their unfortunate circumstance into something very positive. They established a nonprofit organization to assist other victims of identity theft. Their Web site, www.idfraud.net, is available to provide guidance to any identity theft victims across the Nation, and they have devoted themselves to this task.

Identity theft ranges from individual instances like the Hartles involving small or large amounts to large organized professional crime rings. In fact TriWest Healthcare Alliance may well have been the victim of a professional identity theft operation. Like the Hartles, Mr. McIntyre, my constituent, and his company took an unfortunate circumstance, a burglary of their computer in which data was stolen, and turned into a positive model for other companies to follow.

Following the break-in of their Phoenix office and the theft of computer hard drives containing their clients' sensitive personally identifiable information, Mr. McIntyre and TriWest Healthcare Alliance embarked upon an aggressive effort to notify all 562,000 affected customers of the theft. The stolen data included personally identifiable information such as Social Security numbers, birth dates and addresses for military personnel, one quarter of whom were on active duty at the time, retirees and family members, all whom are served by TriWest under a contract with the Department of Defense.

TriWest immediately reported the theft to the police, notified the Department of Defense officials and launched a 30-hour data run to determine what files were stolen. In addition, the company established a dedicated e-mail address and set up toll free telephone

lines with a three-tier response network so that customers would not experience long delays in trying to find out information about the theft and about how it might affect them. TriWest mailed letters notifying victims of theft and provided guidance on steps they could take to protect their credit. TriWest also posted a $100,000 reward for leading to the conviction of those responsible for the theft.

In all, TriWest undertook great efforts to notify victims of the theft at great financial expense to the company. But due to their extraordinary efforts to date no information from the stolen computer files has yet led to a single instance of identity theft.

The nature of identity theft has changed and the threat is more likely than ever to come from breaches of data security, which is why I think this hearing is most appropriate. According to an identity fraud manager at the Federal Trade Commission, there is a shift by identity thieves from going after single individuals to going after mass information. Law enforcement experts now estimate that half of all cases come from thefts of business data banks as more and more information is stored in databases which are vulnerable to attack from hackers.

The Identity Theft and Assumption Deterrence Act of 1998 was an important first step in the road to crack down on identity theft crimes. However, more legislation is needed to protect people from these thieves and from easily obtaining Social Security and credit card numbers, to provide better coordination between victims and credit reporting bureaus, to establish procedures for businesses to follow in the event of a data security breach like we will discuss today, and provide stiffer penalties for those who steal and use other persons' ID.

I look forward to the testimony of the witnesses and help to identify areas in which a legislative response may be needed. I yield back.

[The prepared statement of Hon. John B. Shadegg can be found on page 65 in the appendix.]

Chairwoman KELLY. Ms. Hooley.

Ms. HOOLEY. Thank you, Madam Chairwoman and Mr. Chairman. I appreciate the Chairs and ranking members of both subcommittees in putting together today's hearing and look forward to hearing more about our Nation's data protection. This is an important hearing and hopefully it will be the first of many hearings on the issue of identity theft. It is the fastest growing crime in the United States. I know through these and other hearings we will not only learn about the challenges in fighting identity theft, but also hear unique and effective suggestions on how we in Congress can better protect our consumers and financial institutions from this crime.

I know I can speak for everyone on the Financial Services Subcommittee when I say we are hear to listen with open minds and to put whatever work is necessary into solving this problem. This truly is a bipartisan issue, and in that regard I would like to thank Mr. LaTourette from Ohio for working so closely with me on legislation on identity theft that is nearly ready for induction. I would also like to thank Mr. Frank and all the members of the Demo-

cratic Task Force on Identity Theft for pledging to work together on this issue.

In order to protect both consumers and industry, we all certainly have our work cut out for us. But if the cooperation and dedication of people like Mr. LaTourette and Mr. Frank and the members of both subcommittees are any indication, we on the Financial Services Committee are up to the challenge.

Thank you again, and I look forward to today's proceedings and look forward to hearing from the panelists. Thank you.

Chairwoman KELLY. Mr. Hensarling. Mrs. Maloney just left. Mr. Matheson. Mr. Barrett. Mr. Ford left. Mr. Lucas. Mr. Tiberi. Mr. Feeney.

I will introduce our first panel: Mr. Tim Caddigan, the Special Agent in Charge of the Financial Crimes Division of the United States Secret Service, accompanied by Robert Weaver, Deputy Special Agent in Charge of the New York Field Office; James Farnan, Deputy Assistant Director of the Cyber Division in the FBI; and Mr. J. Howard Beales, III, Director of the Bureau of Consumer Protection in the Federal Trade Commission.

We look forward to having you here today, and we look forward to your testimony. We will begin with you, Mr. Caddigan.

**STATEMENT OF TIM CADDIGAN, SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, UNITED STATES SECRET SERVICE, ACCOMPANIED BY ROBERT WEAVER, DEPUTY SPECIAL AGENT IN CHARGE, NEW YORK FIELD OFFICE**

Mr. CADDIGAN. Thank you. Chairman Bachus, Chairwoman Kelly, Congressman Sanders, Congressman Gutierrez and members of both subcommittees, thank you for inviting me to be part of this distinguished panel and the opportunity to address the committee regarding the Secret Service efforts to protect our Nation's financial and critical infrastructures. Let me also take the opportunity to thank Chairman Oxley, Congressman Frank and all the members of the full committee for their long-standing support of the Secret Service and the interest this committee has conveyed in our mission, our programs and our employees.

With me today is Mr. Bob Weaver, Deputy Special Agent in Charge of the Secret Service's New York Field Office and head of the New York Electronic Crimes Task Force. I am also pleased to be here with my colleagues and partners in fighting identity crimes and related computer crimes from the Federal Trade Commission and the FBI.

In my full statement for the record I provided an overview of the Secret Service's investigative mission and our historic responsibility for safeguarding our currency and financial infrastructure. The Secret Service has statutory jurisdiction to investigate a wide range of technology based crime, including credit and debit card fraud, identity theft, false identification fraud, counterfeit currency and checks, financial institution fraud and telecommunications fraud. These investigations are pursued through our 134 domestic offices with additional support from our 20 foreign offices.

There is no shortage of information, testimony or anecdotal evidence, regarding the nature and variety of cyber based threats to our banking and financial sectors and the need to create effective

solutions. There is, however, a scarcity of information regarding successful models to combat such crime in today's high tech environment. One such successful model is the New York Electronic Crime Task Force and the valuable formula this task force has developed and applied to the prevention and detection of computer based crimes.

Our New York task force has brought together 50 different Federal, State and local law enforcement agencies as well as prosecutors, academic leaders and over 100 different private sector corporations. The task force investigates substantial electronic criminal activity involving e-commerce frauds, identity crimes, telecommunications fraud, and a variety of computer intrusion crimes which affect a number of infrastructures.

Since 1995, the New York task force has charged over 1,000 individuals with electronic crimes and the loss to Social Security exceeding $1 billion. It has trained over 60,000 law enforcement personnel, prosecutors and private industry representatives in the criminal abuses of technology and how to prevent them. The task force has identified tools and methodologies that can be employed by our partners to eliminate potential threats to their information systems.

We consider the New York task force to be the 21st century law enforcement model that modernizes criminal justice and incorporates partnership and information sharing within its core competencies. Accordingly, Congress authorized the Secret Service in the U.S.A. PATRIOT Act of 2001 to expand our task force initiative to cities and regions across the country. We have since established electronic crimes task forces in Los Angeles, San Francisco, Chicago, Boston, Charlotte, Miami, Las Vegas and Washington, D.C..

Our task force model stresses prevention through partnership. We focus on the mitigation of damage and the quick repair of any damage or destruction to get the system operational as soon as possible after an intrusion occurs.

Let me mention one critical point about our partnerships with other law enforcement agencies, academia and private sector. Partnerships cannot be legislated, regulated nor stipulated. Partnerships are voluntarily built between people and organizations that raise the value in joint collaboration towards a common end. They are fragile entities which need to be established and maintained by all participants and built on a foundation of trust. I cannot overstate the significance of these trusted partnerships to the success of our task force model.

Let me share with you some insights regarding a recent ongoing case which our Omaha office is investigating in conjunction with our Chicago, New York, and San Francisco task forces. The case which came to our attention early February through our contacts in the credit card industry involves an unlawful intrusion into the computer system of a third party credit card processor, the companies responsible for processing credit card transactions of companies such as Visa, Master Card, American Express and Discovery. We believe that multiple machines combined to attack this processor's computer system and unlawfully seized millions of credit card numbers along with expiration dates from the company's filings. Our investigation with the FBI determined that these mul-

tiple servers were located both within and outside the United States. The Secret Service is completing electronic forensic examinations and is working with foreign authorities in gathering further evidence concerning this attack.

I want to conclude my statement by again thanking the members of both subcommittees and the full committee for their strong support of the Secret Service and our investigative mission.

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

Chairwoman KELLY. Thank you very much, Mr. Caddigan. Mr. Farnan.

**STATEMENT OF JAMES FARNAN, DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION, FBI**

Mr. FARNAN. Good morning. I would like to thank the Chairs of both subcommittees as well as the other members for their opportunity to testify today. Holding this hearing demonstrates your commitment to improving the security of our Nation's information systems and this committee's leadership on this issue.

My testimony today will address the activities of the FBI's Cyber Division as they relate to a broad spectrum of cyber criminal acts.

Last week a headline in the Atlanta Journal Constitution announced Hackers Strike Georgia Tech Computer, Gain Credit Card Data. The article goes on to discuss the information on 57,000 people that was available to the hackers, including about 38,000 credit card numbers. The university had moved the database from one system to another but it failed to put up a fire wall to protect the data.

Incidents like this happen every week, even to organizations at technology's leading edge like Georgia Tech. American consumers and businesses are increasingly relying on the Internet. E-commerce is growing in all sectors of the U.S. economy. Although most e-commerce transactions are business to business, e-commerce retail sales in the United States reached $46 billion last year, up from $36 billion in 2001.

When Internet users, be they businesses or consumers, are impacted by Internet crime, the viability of e-commerce is compromised. When a cyber crime is committed, the FBI is in a unique position to respond because it is the only Federal agency that has the statutory authority, expertise and ability to combine the counterterrorism, counterintelligence and criminal resources needed to effectively neutralize, mitigate and destruct illegal computer supported operations.

The FBI's reorganization of the last 2 years included the goal of making our cyber investigative resources more effective. In 2002 the reorganization resulted in the creation of the Cyber Division where we have taken a two-tracked approach to the problem. One avenue is identified as traditional criminal activity that has migrated to the Internet, such as Internet fraud, online identity theft, Internet child pornography, theft of trade secrets and other similar crimes.

The other nontraditional approach consists of Internet facilitated activity that did not exist prior to the establishment of computers, networks and the World Wide Web. This encompasses cyber ter-

rorism, terrorist threats, foreign intelligence operations, and criminal activity precipitated by illegal computer intrusions into U.S. computer networks, including the disruption of computer supported operations and the theft of sensitive data by way of the Internet.

The FBI assesses the cyber threat to be rapidly expanding as the number of actors with the ability to utilize computers for illegal harmful and positively devastating purposes is on the rise. A typical case will come to the FBI through the Internet Fraud Complaint Center, which later this year will be renamed as the Internet Crime Complaint Center to more accurately reflect its mission. In its fourth year of operation the Center has proven to be a very successful clearinghouse, receiving over 75,000 complaints last year on crimes ranging from identity theft and computer intrusions to child pornography.

If the Center, for example, received an intrusion report from a company in, say, Birmingham, Alabama, we would first attempt to locate where the intrusion took place. That same company may have its servers in Minneapolis while the intruder is routing through California and Europe. If the servers in Minneapolis were hacked, the Minneapolis Cyber Crime Task Force would be assigned to lead the case. The leads in California could end up in Eastern Europe, Nigeria or even back in Birmingham if an insider were involved. One of the FBI's response teams would be called upon to preserve evidence and that evidence would be forwarded to one of our new regional computer forensic laboratories now located in Chicago, Dallas, and San Diego. Simultaneously other FBI computer experts would determine the extent and duration of the intrusion and whether the attacker came from inside or outside the company. Depending on the sophistication of the intruder, the case may be solved in a few days or it may take years.

Cases are routinely complex and often involve international connections. Cyber crime continues to grow at an alarming rate and security vulnerabilities contribute to the problem. We will soon begin staffing a public-private alliance unit within the FBI which will work with administrators and security professionals to reduce opportunities for criminals by employing best practices and patching vulnerabilities before they can be exploited. Through that unit's efforts combined with the efforts of those in this committee problems like the hacking experience by Georgia Tech will happen much less frequently. The FBI will continue to pursue cyber criminals as we try to stay one step ahead of them in the cyber crime technology race.

I thank you for your invitation to speak today. I on behalf of the FBI look forward to working with you on this very important topic.

[The prepared statement of James E. Farnan can be found on page 98 in the appendix.]

Chairwoman KELLY. Mr. Beales.

## STATEMENT OF J. HOWARD BEALES, III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. BEALES. Thank you, Chairman Kelly and members of the committee. I am Howard Beales, Director of the Federal Trade Commission's Bureau of Consumer Protection. I am pleased to present the views of the Commission this morning.

The Federal Trade Commission works to prevent and protect information security on a number of fronts. We take law enforcement actions, we provide victim assistance when security breaches result in identity theft. We educate both consumers and business and we hold public workshops to examine emerging issues.

In our traditional role as a law enforcement agency the FTC has brought civil actions to enforce privacy promises, including cases where companies failed to take adequate security precautions with consumers' personal information. When an information breach is reported, the FTC staff activates our protocol for triaging the breach. We evaluate the incident on a number of levels, including the extent of the breach and the type of information that was exposed. We also analyze any jurisdictional issues. We do not have jurisdiction over banks and common carriers, for example. In addition, we determine whether there is an ongoing criminal investigation, given that the breach may involve an underlying theft of information. We coordinate any FTC investigation with criminal authorities because we don't want to get in the way of an ongoing criminal investigation.

When the Commission determines that law enforcement action is appropriate we have two valuable tools to work with. First, section 5 of the FTC Act, which prohibits unfair deceptive acts or practices such as misleading promises about information security; second, starting in May of this year, the Commission will enforce the Gramm-Leach-Bliley Act safeguards rule for the financial institutions within our jurisdiction.

Last August the Commission announced a settlement with Microsoft regarding misleading claims about the information collected from consumers through its passport services. The Commission's complaint alleged that Microsoft misrepresented the privacy afforded by these services, including the extent to which Microsoft kept the information secure.

Microsoft is an important case because it involved alleged misstatements about the security provided for millions of consumers' sensitive information. In addition, it held Microsoft to its security promises even in the absence of a known breach of the system. Thus, the Commission found even the potential for injury actionable when sensitive information and security promises were involved and when the potential for injury was significant.

The Microsoft case was followed by the Commission's case against Eli Lilly. The Lilly case involved alleged misrepresentation regarding the security provided for important information. Like Microsoft, Lilly made claims that it had security measures in place to protect the information collected from consumers on its Web site. As in Microsoft, the Commission charged Lilly with failing to have reasonable measures in place to protect the information. The order in the Lilly case prohibits the misrepresentations and as in Microsoft it requires Lilly to implement a comprehensive information security program.

It is important to note that the Commission is not simply saying gotcha for security breaches. Although a breach may indicate a problem with a company's security, breaches can happen even when a company takes all reasonable precautions. In such instances the breach does not violate the laws that the FTC enforces.

Instead, the Commission recognizes that security is an ongoing process using reasonable and appropriate measures in light of the circumstances. That is the approach the mission took in these cases and in its Gramm-Leach-Bliley Act safeguards rule, and it is the approach we will continue to take.

As I mentioned earlier, in May the Commission's Gramm-Leach-Bliley Act safeguards rule takes effect. The rule requires financial institutions under our jurisdiction to develop and implement appropriate physical and procedural safeguards to protect customer information. The rule takes a flexible approach, requiring greater security measures for the most sensitive consumer information. It requires companies to assess the risks they face, take reasonable and appropriate steps to reduce those risks. Companies must also monitor their security performance and adjust their programs as the risks they face change over time.

The FTC also plays a role in improving information security and in reducing risks to personal information by fostering dialogue and educating the public on security issues. For example, the Commission held a workshop last May to examine the security of consumer information, both as maintained by consumers on their own computers and by businesses on their systems. In May and June of this year the Commission will host workshops that focus on the role of technology again for both consumers and businesses.

The cases of TriWest and Teledata communications Inc., in which massive numbers of individuals' personal information was taken are good examples of where the Commission carried out its traditional education and assistance role. The staff provided advice to those companies on how to notify the affected individuals and what steps those consumers should take to protect themselves.

From these experiences and others the FTC has developed a response kit for businesses which have suffered information security breaches. The kit tells businesses what steps to take to respond to a breach and includes a form letter for notifying the individuals whose information has been taken. These kinds of information security breaches place substantial costs on individuals and businesses. The Commission is committed to reducing these breaches as much as possible through its civil law enforcement authority and its education and assistance programs.

Thank you for holding this hearing, and I look forward to your questions.

Chairwoman KELLY. Thank you, Mr. Beales. I also want to note that we invited Dr. William Winkenwerder, the Assistant Secretary of Defense for Health Affairs at the Defense Department to discuss the DOD's role in mitigating the impacts of a theft at TriWest. Unfortunately, he had already accepted an invitation to testify about this before the Senate Finance Committee right now and his deputy is on travel.

Dr. Winkenwerder submitted a statement for the record and with the members' unanimous consent I want to enter it into the record at this time.

[The prepared statement of William Winkenwerder can be found on page 145 in the appendix.]

Chairwoman KELLY. We thank all of you and I would like to begin with you, Mr. Caddigan, asking you a couple of questions. We

commend the entire Secret Service and especially the agents in the New York Field Office for your truly dedicated and outstanding service to this country. We in New York are understandably very proud of the tenacity of the New York Field Office as it recovered from the destruction of its offices at 7 World Trade Center.

I would like to ask if your task force and the stronger emphasis on information security since 9/11 has led to law enforcement successes?

Mr. CADDIGAN. Madam Chairwoman, I think it is safe to say yes, the proactive approach that the task force model in New York takes with regard to partnering with businesses, it gets on the front end of an issue. We help establish self-assessment vulnerabilities in a particular entity. We can help mitigate those on the front end. We can help develop a response plan for that business should they be victimized. So do those actions prevent activity or help mitigate that in the long run? Yes, ma'am, I would say that it does.

Chairwoman KELLY. That is very good to hear.

Mr. Farnan, your testimony discusses two cases in which the hacker was arrested overseas. How often are hacking cases originated from an overseas point? Do you want to answer that?

Mr. FARNAN. Much more frequently than we might care to think about. What we have learned and the model we come from in law enforcement is to typically think along State jurisdiction lines and the FBI, of course we think when violations may cross State jurisdictional lines. With the advent of the Internet and the World Wide Web, we have to completely reevaluate those jurisdictional lines. We now have to think of the entire planet as a ground or platform from which perpetrators can act, and so we do see a lot of activity from persons based in overseas countries or outside the United States.

Chairwoman KELLY. Mr. Caddigan, do you want to address that?

Mr. CADDIGAN. I think crime has become global in nature, especially with the onset of the Internet and computer. What can take place in a criminal activity in California can almost instantaneously have the victim be victimized in Asia, for example. So we do look at things as a borderless society with regard to fighting crime. We do partner not only domestically with business and law enforcement, but I think it is also as critical to partner in the foreign arena with foreign businesses, foreign law enforcement and governments.

Chairwoman KELLY. Mr. Farnan, is the FBI concerned that large scale hacks or the denial of service attacks might be an instrument of international terrorism?

Mr. FARNAN. We are definitely concerned about that. In the Cyber Division what we have done is aligned our priorities along with those of the FBI. So counterterrorism is our number one priority and our number one focus followed by counterintelligence matters and then criminal matters in terms of our third priority. So we are definitely concerned about that. And we have seen, for example, terrorists who are interested in communicating by way of the Internet, like in many cases we all are. So we pay special attention to that arena.

There are two other sort of elements that help us focus on that. One is that in the international arena especially. We have our legal attache program that is located in about 46 countries, I believe it is, and we are going to start in the Cyber Division an Internet, or we have started an international investigative support unit to work with our legal attaches to make sure that we are addressing that very issue.

Chairwoman KELLY. Good. Thank you, Mr. Farnan.

Mr. Beales, can you give me more details? You mentioned that you have taken some specific measures with the FTC to—what measures, specifically, did you take with respect to the three cases to help the victims?

Mr. BEALES. Well, what we did was to discuss with the companies the kind of a letter they might send and make discussions about the letter. We have a booklet that is consumer information about identity theft that is called Identity Theft: When Bad Things Happen to Your Good Name. And we make that booklet available and encourage companies to provide that booklet to consumers in need of information about what they should do next.

Chairwoman KELLY. Thank you. I am about out of time.

Mr. Farnan and Mr. Caddigan, I want to be sure, we want to be sure, we need to be sure that there is no unnecessary overlap or redundancy between the two of your agencies. I wonder if you would be willing to clarify your authority over cyber intrusions.

Mr. FARNAN. Again we have our—well, the fact that Mr. Caddigan and I are sitting next to each other and Dennis Holly, who is sitting next to me is an agent actually assigned to FBI Headquarters, resources permitting, I want to assign an FBI agent to Secret Service Headquarters, I think we are working in an extremely cooperative and complementary fashion. There is enough crime, as I think you can sort of define from the testimony today, to go around. There is plenty of work to do. And with that, I think that our efforts complement each other. We have specific mechanisms in place to make sure that happens, including the sharing of personnel back and forth.

When it comes to intrusions, the one unique thing that we may bring is the fact that if it is a State-sponsored or foreign government who is trying to break into or hack into a system in the U.S., it is one kind of unique area that the FBI may bring to that. What we have done successfully is work on a case-by-case basis at the field level all the way through the headquarters level to make sure we are not duplicating and complementing efforts.

Chairwoman KELLY. Mr. Caddigan, are you satisfied with that answer?

Mr. CADDIGAN. I would concur completely. We recognize that any single entity can't handle this problem alone. By working together, combining our resources, combining our approach methodologies, we do provide a better product to the public we serve.

Chairwoman KELLY. So you feel that there is not a problem with overlap there?

Mr. CADDIGAN. I think, as Mr. Farnan mentioned, we detailed an Assistant Section Chief to the Cyber Division in headquarters, so conflict is not an issue. We do coordinate at the local level with our task forces. The Bureau has representation and membership in

each of our electronic crimes initiatives throughout the country and, conversely, in smaller environments where we are not present we have membership in their initiatives.

So I would suggest to the panel that the cooperation does exist at the highest level and although there maybe some appearance of overlap it does mesh well together.

Chairwoman KELLY. Thank you. I am out of time. Mr. Gutierrez.

Mr. GUTIERREZ. Thank you very much. First of all, I want to thank Mr. Weaver and Mr. Caddigan and Mr. Farnan and all of those that work with you at the FBI and Secret Service for the work that you do.

I would like to ask Mr. Beales, I guess my concern is what are the responsibilities of financial institutions that suffer from intrusions to their client base in terms of information from them? Is there a 48-hour, 72-hour window, a week, 30 days? Is there something that says you must do this by the FBI's call, the Secret Service knows, they are investigating how long does it take and is there anything that says they have to do it in a specific amount of time?

Mr. BEALES. There is no specific requirement either to give notice or to give notice within a certain period of time. Notice is clearly appropriate in many circumstances and is clearly the best practice and was what we have generally seen in most cases that involve breaches. There are some cases though where notice may not be as useful. And I think in the case of the credit card hack that got the information about credit cards, providing that information to the financial institution so they could block fraudulent activity on those cards is a more effective way to address the problem and considerably reduces the need for notice to consumers.

Mr. GUTIERREZ. So I guess then what you are saying is we have to rely on the credit card companies and the service that is provided to protect the consumer but we are not—we don't necessarily inform the consumer so that he can help protect himself and you think there might be just best practices where the consumer is left totally out of the picture and unaware? It seems to me the credit and the reputation belongs to the consumer and that credit and reputation is I trust—I entrust it to the financial institution, to my credit card company, my mortgage company and that they have a responsibility to me to alert me. I mean, if my bank didn't call me because somebody ripped off my money from my checking or bank account immediately, I think I would get pretty angry about it. I guess my question is don't you think there should be some best practices established so that consumers can help themselves?

A booklet is nice and I am very happy that you issue that booklet, but at what point do we trust the consumer to engage and to cooperate with the Secret Service, with the FBI, with the District Attorney's office or whatever it is that is prosecuting the case. What do you think?

Mr. BEALES. I completely agree with you that consumers need to find out in most of these cases. And we have—in the particular cases that are at issue here we have strongly encouraged the companies to provide information to consumers and try to make it easier for them to do that. I think there is no question that is the best practice in most cases.

Mr. GUTIERREZ. So the best practice is trust the companies to figure out when they should inform the consumer that their credit has been somehow hurt or compromised and that somebody has access to their information; we should just trust the companies to do this?

Mr. BEALES. We don't have regulatory authority.

Mr. GUTIERREZ. Who does?

Mr. BEALES. I am not sure that there is any agency that has authority to.

Mr. GUTIERREZ. So there is no authority that you understand that anyone has?

Mr. BEALES. There is authority and there are regulations both by us and the bank regulatory agencies that govern the front end, that require financial institutions to have in place measures to prevent breaches of information security and to take appropriate steps in order to keep that from happening in the first place.

Mr. GUTIERREZ. I understand that. And I guess then that maybe we should look at how it is ultimately the House of Representatives or legislatively we deal with the issue given that it is your testimony that there is no best practice other than let the companies figure out how it is they should deal with the consumers, but there is no 72 hours, 48 hours. So we probably may need some best practices established to protect the consumer because in the end that is who we have to protect and that is who is most hurt in this situation.

Again, I want to thank the members of the Secret Service and the FBI for their work because I know they have a lot of work, especially after September 11th. I want to thank them for all the hard work that they do. I want to thank folks at the Federal Trade Commission, too. You do a great job there, too.

I wanted to see if we could figure out what we might need to do, this committee and other committees. Thank you all so much for your testimony this morning.

Chairwoman KELLY. Thank you, Mr. Gutierrez.

Mr. Bachus.

Mr. BACHUS. Thank you. Mr. Beales, will the FTC be taking a closer look at banks' third party providers with respect to the service providers information security programs?

Mr. BEALES. It is something that we are very interested in, in looking at security cases and information security cases in general. It is an area where the bank regulators also under their safeguards rules also have authority and it is a place where we would want to coordinate with the bank regulatory agency as to who was in the best position to address any particular case.

Mr. BACHUS. Are you already doing that? Are you already looking at these?

Mr. BEALES. We talk to the bank regulatory agencies on a very regular basis about a host of issues, including this.

Mr. BACHUS. How about the bank's third party providers? Are you all in contact with them or are you reviewing their information security programs?

Mr. BEALES. Well, we have—under the FTC rules we can't talk about particular investigations. They are not public.

Mr. BACHUS. I don't want specifics, but is it a part of your general procedure? Do you——

Mr. BEALES. Well, in our general procedures we are sort of looking for cases everywhere. They may come from reports in the media and they may come from complaints. They may come from referrals from other law enforcement agencies, and if they are in our jurisdiction and third party service providers, we would be very interested in pursuing.

Mr. BACHUS. Banks' third party service providers are within your jurisdiction, aren't they, as far as their information security?

Mr. BEALES. Yes, I believe they are. They are also subject to the bank's——

Mr. BACHUS. I understand that. But I am just talking about for a minute—without being specific, have you taken a closer look at any of their information security programs?

Mr. BEALES. We do not have any—we haven't done anything that was specifically targeted to bank third party.

Mr. BACHUS. I understand that. I am not talking about target. I am just saying are there instances when you have reviewed their information security programs?

Mr. BEALES. If we review information, it would be in the context of a particular investigation of a particular company.

Mr. BACHUS. I understand that. I am not talking about particulars, but have you done that? I know you have the right to do it, and you might do it, but have you done it?

I am not going to ask specifics about companies, but I want to know if that is part of your jurisdiction?

Mr. BEALES. It is part of our jurisdiction.

Mr. BACHUS. My question is, are you all taking advantage of it? Are you all doing that? Are you reviewing or have you reviewed any?

Mr. BEALES. We have reviewed cases as they have come to our attention.

Mr. BACHUS. Banks, third-party providers?

Mr. BEALES. Yes, sir.

Mr. BACHUS. Okay. You know, on the DPI case, this information was looked at, but it wasn't actually taken, is my understanding.

Mr. BEALES. I am not—I don't know that for sure.

Mr. BACHUS. Okay. All right.

Are you aware of any identity theft cases that resulted from the DPI hack?

Mr. BEALES. I am not.

Mr. BACHUS. How many personnel are dedicated to investigating pretext calls at your agency?

Mr. BEALES. There probably isn't anyone that is completely dedicated. We are a small agency and people multi-task, but there are—there are four or five staff members who have been involved in pre-texting investigations.

Mr. BACHUS. Let me ask the Secret Service, either one of you gentlemen, Mr. Weaver or Caddigan, in your experience how responsive have credit card issuers and processors been in notifying the Secret Service of data penetrations or other hacking events.

Mr. CADDIGAN. I think, as a general statement, it is safe to say that they have been very responsive. We have ongoing and long-

standing relationships with the credit card companies individually, the banks that they represent, and on occasion the third-party processors as it becomes important for us to deal with them.

Mr. BACHUS. You have been in a position to know whether they are cooperative, and they are?

Mr. CADDIGAN. Yes, sir. They are very cooperative.

Mr. BACHUS. To Mr. Farnan, do you work closely with the private sector in monitoring data penetrations?

Mr. FARNAN. Well, one thing to keep in mind here is that what has happened at the FBI is the former National Infrastructure Protection Center has now migrated to the Department of Homeland Security.

So what is happening is on the vulnerability side of the house, the Department of Homeland Security is really assuming that responsibility. And to focus our limited resources the best we can, we are focusing more on the threat side of the house. By that I mean, who is it out there that is causing the problem.

So to answer your question, we are not directly monitoring.

Mr. BACHUS. You are focusing on the perpetrators?

Mr. FARNAN. Yes, sir.

Mr. BACHUS. In our second panel, we are going to talk about TriWest, what happened there. Now, you know, this hearing has sort of focused on penetrations of data systems, hacking, that nature. But in that case, someone either on the inside, it is an ongoing investigation, or on the outside just walked in and walked away with hard drives containing information on half a million people.

Which obviously, if you had a preference for what you would do, is, you know, go in and try to grab stuff. If you could just walk in and take the hard drives out or the disk out, you know, that would be the preferred method I would think for thieves.

I read the testimony of TriWest's CEO, and it was 2 days before they discovered this theft. From a law enforcement agency perspective, what do you advise corporations that have these large databases of how to protect them from a security standpoint? Not someone hacking, but someone walking in or somebody walking out, whether they walked in or not.

Mr. FARNAN. One of the things that we tend to see is sometimes we do tend to think of these cases as extremely complex, because once when we get into the world of electrons and what is happening in cyberspace, things can get complicated pretty quickly. But in doing that, sometimes we forget the fundamentals, sometimes we forget to lock the door.

So there are times when you have to look at, where does any company or university or institution keep its servers, where do they keep their mainframes, what kind of security, in terms of locked doors, places in the building that kind of equipment is kept. Is it kept on site in the same place as the corporate headquarters or is it secured in an alternate location.

So sometimes even though we get into lots of victims involved in these crimes, and the crimes can be really worldwide in nature, sometimes we forget the very fundamentals. And that is really, probably, the place to start with security matters.

Mr. BACHUS. I totally agree with you. I would think fundamentally you worry about sophisticated—through the network, but you obviously shouldn't—you should just protect the front door.

How about the Secret Service? Any comments you would make?

Mr. CADDIGAN. I would concur.

I think in a proactive approach to information assurance or information security, a company, an organization, an entity needs to be concerned dually, both physical and cyber.

And when you look at vulnerability assessment, an organization can be guided to conduct their own self-assessment, I think you do—those things rise right to the top. I don't know the particulars on this case, but as you describe them you would ask the simple questions on the front end, is there a lock on the door, is there protection on the hard drive, what schedule do you use in order to verify that information has not be compromised.

And again, not having any knowledge of this case, protecting your cyber elements again is just as critical as your physical elements. So it is easy to critique on the back side, but the proactive approach I think might have determined that vulnerability on the front side.

Mr. BACHUS. Thank you.

Chairwoman KELLY. Mr. Caddigan, I want to follow up.

Just one quick question to Mr. Bachus's question, and that is, about the way that the computers contain the information. If people are lifting the hard drives, then it seems to me that containing information that separates numbers from names and Social Security numbers from addresses, things like that can be done. Are you overseeing things like that? Are you looking at things like that, or recommending things like that to companies?

Mr. CADDIGAN. Yes, ma'am. Recommending would be the proper word. We do have issues with regard to—these companies are private sector. We can't mandate, we can't legislate, but we certainly can recommend security mindedness. Those would be exactly the type of things that we would ask you to consider in how you collect and keep your data.

Chairwoman KELLY. Thank you. Ms. Hooley.

Ms. HOOLEY. Thank you. I am going to direct most of my questions to Mr. Beales, but if any of you would like to jump in, please feel free to do so.

I know you are to provide victims assistance and consumer education.

Can you highlight, beyond your testimony specifically, specific steps the FTC has taken in regard to consumer education and victims assistance? Let me explain what I am looking for.

I know in regard to victims assistance you have a centralized database to aid law enforcement. Are there any programs in place specifically to help victims of ID theft clean up their credit, which as many of you know can be a long and expensive process? And do you have any suggestions for new ways to help in this regard? That is the first part of my question.

The second part is, you have to finalize rules which require financial institutions under FTC's jurisdiction to develop and implement appropriate physical, technical and procedural safeguards to protect consumer information.

Can you tell me which financial institutions might be subject to this rule? Would the 400 companies which are sponsored by financial institutions to process credit card payments, such as DPI, be subject to the rule?

Then the third part of my question is, I know your—you have been traveling around the country to educate local law enforcement. I would like to know how well that has gone.

Can you tell us a little bit about the seminars, how many cities have you traveled to, how often are they held, and what might be coming next. And is there anything we can do to help you with that?

I know I have used your brochures extensively for the education piece. Thanks.

Mr. BEALES. When consumers call our hotline for identity theft to report a problem, the phones are answered by trained counselors who will try to talk them through what they need to do next.

Our role is to provide advice to consumers about the steps that they need to take. We do that to the best of our ability, but it is really up to consumers to do that.

There are private programs that will help consumers individually on a one-on-one basis, go through the process of cleaning up their credit. It is not something that we do or would have the resources to do for the complaints we get. We get—last year we had approximately 161,000 victims who contacted our clearinghouse for information and assistance.

Ms. HOOLEY. Let me ask you, are there any other things? I mean, I know what the directions are that you give victims, and it can take 3 or 4 years. I mean, I think the average time is an enormous amount of time to clear up their credit.

Do you have suggestions or ideas, any of you, about how we can make that happen in a much quicker, less costly, less time consuming, less frustrating way?

Mr. BEALES. We are constantly looking for better ways to do it, to make it simpler. We have—I mean that led us last year to put out a uniform affidavit. So consumers could report the fraud on one form and then submit copies to different financial institutions, as one way to try to simplify the process.

We are working—we have been working with the credit reporting agencies to initiate a pilot program that would let consumers just make one call to contact all three credit recording agencies and establish a fraud alert. We expect that program to go into place later this month.

We are continually looking as well for things that Congress might do to make this simpler. At this point we don't have any specific suggestions. But, it is something that we are very much alert to, and looking for ways that we or you or anyone else could make this process less of a hassle for the people who are victims.

As to our Safeguards Rule, there are a wide variety of firms that you wouldn't think of as financial institutions that are or may be financial institutions under the Gramm-Leach-Bliley Act rules that are subject to our jurisdiction and that would be subject to the Safeguards Rule.

Accounting firms that do tax preparation and the like, for example, may well be subject to the rules. Auto companies that provide

credit or dealers that provide credit or financial institutions are subject to the rules.

The third parties that provide services, to banks or anyone else, that involve handling sensitive information would likely be financial institutions and subject to our rules.

It is a hodgepodge of who it is, there is no easy way to describe the universe. But, our jurisdiction is basically any financial institution, except banks or financial institutions that are specifically regulated by some other regulator.

As to the law enforcement training, I believe we did five——

Ms. HOOLEY. Let me finish up that. The companies that are sponsored by financial institutions, like DPI, are they under your jurisdiction?

Mr. BEALES. I believe they are, yes.

Ms. HOOLEY. Okay.

Mr. BEALES. As to the law enforcement training, I believe we did five cities last year. We did training programs in five cities last year. We thought it was successful and useful.

We did those training programs in conjunction with the Justice Department and with the Secret Service and the Postal Inspection Service. We tried to bring in local officials, as well, in each one.

This year we have five more planned in different cities around the country, and we are continuing to pursue that activity.

Ms. HOOLEY. How can we help you in increasing those numbers for law enforcement, because I think that is a really important piece, the law enforcement piece of identity theft.

Mr. BEALES. Well, the—the piece that, I mean, the training piece I mean is simply limited by resources. It is—it is—it takes staff, time and effort. And we have tried very hard to work with the other law enforcement agencies involved to extend our resources and leverage them as much as possible.

Ms. HOOLEY. Thank you.

By the way, thank you for the booklets. We do send out a gazillion of them.

Mr. BEALES. I am glad to hear that.

Chairwoman KELLY. Mr. Shadegg.

Mr. SHADEGG. I am going to pass.

Chairwoman KELLY. Mr. Renzi.

Mr. RENZI. Thank you, Madam Chairwoman.

Just two real quick questions, so then we can go vote.

I am really interested in the who behind all of this. You know, we have heard that there are hackers involved and terrorists involved, organized crime involved, and even insiders. And I know the FBI and the Secret Service has done a wonderful job in foiling some attempts. What can you share with me as far as the who behind this.

I've got a little follow-up question. Thank you.

Mr. FARNAN. First, our experience and our investigative activity to date suggests one thing that really kind of stands out. And that is, that the highest, the person that we are most concerned about is, in fact, the insider as opposed to an outsider. That person poses the most significant threat.

Secondly, what we focused on and what we are concerned about are organized groups that may be attempting to obtain, penetrate

machines and obtain large amounts of data. And we are very concerned, also, about the threats that are posed from foreign countries, frankly.

But, one important point, I think, to emphasize is the fact that it is the insiders. It is the people who have access to the machines and to the data that really pose a significant threat, which raises the question, who watches the watchers?

Mr. RENZI. Well said.

Congressman Shadegg and I share a real concern living in Arizona with the border. We are reminded weekly of the threat, particularly as it relates to terrorism. We recently just had an Iraqi arrested down in the Tucson area. That goes to my follow-up question, which is the market, the black market.

We have probably a sophisticated black market as it relates to credit cards, as it relates to Arizona, drivers' licenses, passports. Los Angeles has a whole market that is even bigger than ours, because of the immigrants that move through our area looking for identification and also the terrorists, I think, that are also looking for that new identity.

Could you talk real quickly then about the driving force of once the insiders or whoever have stolen this information, who they are selling it to, where is the purchasing, the fencers, I guess, is what I am talking about?

Mr. CADDIGAN. The insider threat is—the correlation of the insider is permeated through many of the cases that we have.

The hacking community, the groups out there that do hacking for a pastime, we think they fall maybe into three categories.

One is those doing it for the challenge. They want to show that they can tap into your vulnerability and exploit you.

The second is political, which means they get into websites. They deface them. They put a statement, a logo, again, sometimes just for encouragement.

The other is for profit. So they are the ones that I think we are all concerned about in law enforcement, those that are getting in there and stealing information. We find, in many cases, they make that information available in chat rooms on the webpage.

They indiscriminately make it available to anyone willing to pay for it. Thus, it is hard to track where the sources are going to, because they are everything and anything.

Mr. RENZI. Your answer leads me to believe that there is not an absolute purchaser. There is not an absolute market that you have been able to identify, indiscriminate purchasers?

Mr. CADDIGAN. There is not an absolute market. I think that is safe to say.

With regard to terrorism and the like, we do find—with illegal immigrants, terrorists, those that are truly trying to hide their identify, aren't using it to gain credit or to have purchasing power, they are using it to be able to live and exist with a different name that doesn't draw attention to them.

Mr. RENZI. You are able to set up an electronic fencing operation, a pseudo fencing operation, where you look on the Internet and purchase that information and then go after that individual, just like you would——

Mr. CADDIGAN. That does occur.

We have always had sting operations with regard to, as your concern expressed, the immigrants. We have had some terrorism links to those that are just trying to have different breeder documents, and what they can get out of the breeder documents, meaning passports, driver's license and the like. It is just strictly to have a change of a named identity that they can use at will. So it does run the gamut in that regard.

Mr. RENZI. Let me just thank you all of you for your testimony today, and especially at this time in our Nation's history for the work you are doing.

I know we are talking about incidents that have already occurred today. I can't imagine the amount of incidents that you have foiled. So thank you for that.

Chairwoman KELLY. Thank you very much.

We have just been called for two votes on the floor. So I will eventually deal with that, but I want to note that some of the Members may have additional questions for this panel, that they may wish to submit those questions in writing.

So, without objection, the written hearing record will remain open for 30 days for members to submit written questions and to place responses in the record.

This panel is excused with our great thanks. We appreciate the fact that you gave us so much of your time, and we look forward to being in continual contact with you, because this is quite a thorny issue. Thank you very much.

In light of the vote, I am going to recess this committee for 20 minutes, and we will reconvene in 20 minutes for our second panel. Thank you very much, gentlemen.

[Recess.]

Chairwoman KELLY. As the second panel takes their seats at the witness table, and with the agreement of Members, I want to recognize the gentleman from Arizona, Mr. Shadegg, for the purpose of introducing our first witness before I proceed with the rest of the introductions.

Mr. SHADEGG. Thank you, Madam Chairwoman.

As I mentioned in my opening statement, I have the privilege of having a constituent on this panel.

Mr. David McIntyre is here to testify about the burglary of his company's office located in my Congressional district, the burglary that occurred on the morning of December 14th, 2002, and about the response by his company to that burglary.

Mr. McIntyre is president and CEO of TriWest Healthcare Alliance, which is a private corporation that administers the Department of Defense's TRICARE Program in a 16-State region in the central United States. TriWest is the largest Department of Defense contractor in Arizona.

Mr. McIntyre has more than 18 years of experience in healthcare and healthcare policy and in the healthcare business. He was previously Vice President of Blue Cross Blue Shield of Arizona, which is where I met him.

For our purposes, Madam Chairman, he has 9 years of experience serving on the staff of Senator John McCain. So he is somewhat familiar with the hearing process.

As I mentioned in my opening statement, in the wake of the burglary of TriWest's offices in Phoenix, Mr. McIntyre's company aggressively responded.

Mr. McIntyre personally oversaw and took part in the plan to notify customers about the stolen information and personally telephoned a number of those whose credit card information was stolen.

Mr. McIntyre has turned that negative experience, the burglary of his company's offices, into a positive model for other companies across the country who are victims of information theft.

I appreciate him being here to testify, and I look forward, as I am sure the rest of the panel does to his testimony.

Chairwoman KELLY. Thank you, Mr. Shadegg.

Our remaining witnesses on the second panel are Mr. Kevin D. Mitnick, President and Co-founder of Defensive Thinking and a computer hacking expert. Stuart Pratt, President of the Consumer Data Industry Association. Mr. John Brady, Vice President for Merchant Fraud Control of MasterCard International, and Evan Hendricks, Editor and Publisher of Privacy Times. We welcome you all. We thank each of you for testifying here today.

Without objection, your written statements will be made a part of the record. You will each be recognized for 5 minutes, and if you don't know the color codes on the lights in front of you, the green light is all go, and as soon as you see the yellow light it means it is time to sum up because the red light will come on. We all know what that means.

With that we will start with you, with Mr. McIntyre.

**STATEMENT OF DAVID J. MCINTYRE, JR., PRESIDENT AND CEO, TRIWEST HEALTHCARE ALLIANCE**

Mr. MCINTYRE. Chairwomen Kelly and distinguished members of the Financial Services Committee, thank you for the invitation to appear before you today to discuss the important topic of identity theft.

Congressman Shadegg, thank you for your overly generous and very kind remarks, and I appreciate your long interest, dedication and effective leadership on this critical consumer issue. It, in fact, is an issue that affects every consumer in America, probably a very unique one at that.

As Congressman Shadegg said, my name is Dave McIntyre. I am the president and CEO of TriWest Health Care Alliance. We are a private corporation that delivers health care services to the Department of Defense and its beneficiaries in 16 states. We serve 1.1 million people.

This was a very painful holiday period for me this last year, because like a number of organizations in this country, I have had the opportunity to learn firsthand about the information theft.

What is most appalling to me, however, is that in many cases, it takes the individual who suffers the identity theft longer to clean up their credit report than is the jail term that is served by the criminal who actually perpetrated the act. As a consumer, as a business leader whose company suffered the theft of the personal information of its customers, I am grateful to you for your focus on this critical issue.

On Saturday morning, December 14th, one of our offices was burglarized. Computer equipment and data files containing confidential and personal information of more than 570,000 members of the military, their dependents and retirees was stolen.

The information on the stolen hard drives included names, addresses and Social Security numbers, which we are required by the Federal Government to collect, along with other personal information. Fortunately, it only contained 23 credit card numbers.

I was told by experts shortly after the theft that the most effective thing I could do was to get out in front of this issue and notify consumers as quickly as possible. So that is what we set out to do. We notified authorities on learning of the theft.

Secondly, we contacted our DOD partners to jointly create and implement a comprehensive three-pronged action plan to protect our beneficiaries. We went to the media. Because many of these people were away from home during the holidays visiting their families. We wanted to make sure that we lost no time.

The military worked through their chain of command and notified every installation worldwide, so that we would reach the leadership and all of the folks serving in the military.

We sent the first of what will now be three letters to the individuals who were affected, to notify them of what had occurred, and give them advice based in part on the counsel of the FTC on what they could do to protect themselves.

This has been a joint effort, working with Dr. Winkenwerder, the Assistant Secretary of Defense for Health Affairs, the Surgeon General of each service and all of the command structure in the military. It has been a fabulous partnership, albeit at a time when they didn't have time to spend on this issue.

Third we posted a $100,000 reward to aid law enforcement in their efforts to try to detect who had done this. As you can imagine we were devastated by this event. However, we focused all of our energy on trying to do what we would want to have done were we the consumer who was sitting on the other side.

Given the burden on the individual of placing a fraud flag with three different credit bureaus, we worked with the credit bureaus to develop a plan that has allowed us to request on the behalf of our customers, not forcing them to do it, the actual request of a fraud flag.

To date, more than 63,000 of the people on that list have chosen that option, and we have done that work on their behalf.

Through this experience, I have learned a lot. I never planned to become an expert or even close to someone who knew a lot about the issue of information theft. I am pleased to be joined by a number of other people who obviously know a lot about this topic as well.

I have come to believe that the work that was done by Congressman Shadegg needs to be built on in a couple of ways.

First, I think that every leader of any organization, whether it is public or private, has an absolute obligation to their customers, that when that information is compromised, they have an obligation to inform their customer of the fact that has happened. It is painful. It is awkward. It is embarrassing. It is expensive. But you

know what, it is not our information, and unless you arm the consumer with that information, they cannot protect themselves.

Second, as a consumer, I have observed the inconsistencies in the last 4 months with how my credit card information is handled. Half of the receipts from restaurants have the full credit card number and authorization date or expiration date posted on it. That is all you need and a name to go to the Internet and buy something.

In addition, I still belong to the Senate Credit Union. I went to the credit union to find out what comes on your statement. Social Security numbers are printed on those documents if you go and ask for the balance on your account today. Same is true in the House Credit Union.

So we need to work to look at when is it necessary to have the full Social Security number printed on the document, when is it necessary to have the full credit card number printed.

I also think that penalties in this area for those who perpetrate such crimes need to be looked at and significantly enhanced.

Fourth, I believe that credit bureaus should allow organizations to act on behalf of their customers, and that they should establish consistent timelines for the updating of fraud flags.

Thanks for the invitation to be before you today. I hope that this is the year that you are able to take the incidents that we have all faced and use them as leverage to further protect consumers in this country. I look forward to answering any questions you may have.

Thank you, ma'am.

Chairwoman KELLY. Thank you.

[The prepared statement of David J. McIntyre can be found on page 114 in the appendix.]

Chairwoman KELLY. Mr. Mitnick.

**STATEMENT OF KEVIN D. MITNICK, PRESIDENT AND CO-FOUNDER, DEFENSIVE THINKING**

Mr. MITNICK. Good morning, Chairwoman Kelly, Chairman Bachus and distinguished members of the committee.

My name is Kevin Mitnick. I appear before you today to discuss your efforts to review current industry practices concerning security procedures for the prevention of electronic theft of credit card information and identity theft.

I am primarily self-taught. My hobby as an adolescent consisted of studying methods, tactics and strategies for circumventing computer security, and for learning more about how computer systems and telecommunications systems work.

I have 15 years experience circumventing information security measures, and I can report that I have successfully compromised all systems that I targeted for unauthorized access except one.

I also have 2 years experience as a private investigator with responsibilities that included locating people and assets using social engineering techniques. Social engineering is the same thing as pre-texting that Mr. Bachus spoke to earlier.

I have gained unauthorized access to computer systems at some of the largest corporations on the planet and have successfully penetrated some of the most resilient computer systems ever developed. I use both technical and nontechnical means to obtain source

code to various operating systems and telecommunication devices to study their vulnerabilities and their inner workings.

Currently, I am the Co-founder of Defensive Thinking, a Los Angeles based information security firm. I recently co-authored with William Simon a book titled the "Art of Deception," published by John Wiley and Sons, which has become an international best seller. The book details nontechnical methods and tactics, in essence pre-texting, that computer intruders use to compromise valuable information assets, including credit card information.

Social engineering is a method where the intruder deceives his target into complying with the request based on false pretenses and psychological manipulation.

It is important to understand, and all companies and their employees need to realize, that the most insidious vulnerability to information security are the well-meaning, hard-working folks that use, operate and maintain information systems.

The prevention and detection of social engineering attacks should not be ignored or underestimated. In fact, the majority of scams involving identity theft and credit card fraud include social engineering on some level.

In an attempt to deter carding, many retailers are now requiring an on-line customer to provide the three-digit CVC number that card issuers have begun to use.

But the thieves also obtain the CVC number. With it, he is able to use the information to commit fraud against unsuspecting cardholders and merchants. I understand that the subcommittee will be examining three recent cases involving large-scale thefts of nonpublic, personal identifying information and credit card details.

A major part of the problem is that the criminals only need to obtain information that is stored or processed in thousands of computers systems around the world. In February of 2003, DPI, a credit card processing services company, reported that an unknown intruder had compromised their network and gained access to a database that held over 8 million credit card accounts.

DPI did not release any details describing how the breach occurred, citing cooperation with Federal law enforcement officials. The DPI case was widely reported in the press because of the astounding number of credit cards potentially compromised.

But when examined closer, you will realize that these types of attacks happen all the time. In my opinion, the committee should not overlook that many similar attacks on networks containing financial information are not detected by the owner or operators. It is important to realize that many of these security incidents remain undetected because of poor security and auditing practices.

DPI has publicly claimed that the intrusion occurred from the outside of the organization. Although, I do not like to hypothesize on facts and circumstances of an any attack without details, I would recommend that DPI consider the possibility that the attacker had assistance from the inside of the company.

Every day the security community announces new vulnerabilities and operating systems in application software that have been identified. Vulnerabilities in software can be exploited to gain remote access to the target computer. Many system programs contain programming errors that enable the intruder to trick the software into

behaving in a way other than which is intended in order to gain unauthorized access rights, even when the application is part of the operating system of the computer.

Once a new vulnerability is recognized, the software developer releases a patch, a modification to the software that might be installed by individual companies, a process that may be overlooked for days, weeks, months, even years. Meanwhile companies using that software remain vulnerable or are forced to disable or block access to the vulnerable service until the patch becomes available.

Even then in many cases this is not enough. There are a number of sophisticated hackers who are able to discover previously unrecognized security vulnerabilities and then use them to compromise global computer systems and networks.

I agree that it is essential to implement security strategies to prevent, detect and respond to security threats and attacks, but it is too easy to look in the wrong direction for an answer. In my view, attempting to solve the complex problem by micromanaging every on-line site that accepts credit card transactions would turn out to be wasteful, inefficient and not a very successful exercise.

Instead, I recommend that the committee look into a different direction. I recommend that you explore mitigation strategies which focus on improving the authentication of the credit card user. In any on-line credit card transaction, identity and authorization is based on the information a consumer provides to the merchant. This is no better than a static password.

There is an old saying among hackers. You never know if someone else has your password. The reality is that a password or its equivalent is too easy to steal. A first step towards a solution would be to strip away the identity value of all personal information.

If knowledge of a credit card number, expiration date and the corresponding customer name and address is without value, stealing this information would be a useless to an imposter.

Unfortunately, authentication technology has not yet matured to the point of being able to provide an easy solution to the issue. If not being done already, I would recommend that the finance industry explore additional authentication methods that may include digital certificates, identification of the user's location based on IP address or telephone number, or verification of a PIN through a separate communications channel.

For example, consider this scenario. You have just placed an Internet order for a new cell phone with a price tag of several hundred dollars, and placed an on-line order with your credit card information, but you were not required to give a PIN number. Instead, you next dial your credit card company, and when prompted you enter your card number. An automated system then reads off the details of the transaction. You are satisfied that the details are correct. The system tells you: To authorize this transaction, enter your PIN number.

What would be the advantage of this approach? The thousands upon thousands of individual retailers would not have access to consumer PIN numbers. The fact that so many retailers store the credit card numbers of on-line customers gives rise to the kind of credit card theft that this hearing is addressing.

If they also store the customer PINs, then there is no gain in security. The PIN becomes almost worthless as a security element. But under the approach I have suggested, only the bank would have access to the PIN number information. Under this arrangement, the theft of the card numbers would be of limited value.

In another area, I would also recommend consumer-awareness training programs that educate people about the various scams being used to steal their credit card details and personal information, a practice that can prove highly valuable to effectively minimize identity theft and credit card fraud.

I believe that all on-line retailers who accept credit cards should be encouraged or required to do the following:

One, perform a regular, thorough risk assessment on their information assets, especially systems that process or store consumer financial and personal information.

Two, implement policies, procedures, standards and guidelines as dictated by the results of the risk assessment.

Three, create an audit and oversight program that measures compliance. The frequency of the audits ought to be determined consistent with the mission. The more valuable the data, the more frequent the audit process.

Develop a process to ensure meaningful and effective patch management for all computer systems. Employ authentication methods that do not use nonpublic personal identification information, such as a mother's maiden name, birth date, birth place, driver's license number, address, phone number or Social Security number.

Next, effective audit procedures implemented from the top down must be part of an appropriate system of rewards and consequences in order to motivate system administrators, personnel managers, and employees to maintain effective information security, consistent with the goals of this committee.

Next, establish a security-awareness training program designed to educate their employees on the threats to information security and to change employee behavior to foster a secure environment. These would follow the security recommendations described in detail in my book, "The Art of Deception."

In terms of legislation, I recommend that the subcommittee consider the following:

One, legislation that prohibits merchants or credit card processors from electronically storing PINs or other types of verification credentials such as the CVC, unless it is essential to business needs.

Two, the requiring of periodic security assessment and or penetration testing to evaluate the security posture of any business that stores or processes credit card transactions, to be performed by an independent information security consulting firm.

Three, require encryption of stored financial or personal information. If this was done by TriWest or by DPI, then the information would not be accessible to the hackers.

Finally, I want to offer what I have deemed the most important factor in security, the human factor. This is essential, underlying all security issues, whether it is from deceptive credit card thieves or terrorist operatives to blend into our communities.

I believe it is essential to consider regulations that mandate security awareness training as part of an overall security program as required by HIPAA and the GLBA.

Thank you.

Chairwoman KELLY. Thank you very much, Mr. Mitnick.

[The prepared statement of Kevin D. Mitnick can be found on page 124 in the appendix.]

Chairwoman KELLY. Mr. Pratt.

**STATEMENT OF STUART PRATT, PRESIDENT CONSUMER DATA INDUSTRY ASSOCIATION**

Mr. PRATT. Chairwoman Kelly, Chairman Bachus, members of the committee, thank you for this opportunity to appear before you today.

For the record, I am Stuart Pratt, president of the Consumer Data Industry Association, and we commend you for holding this hearing on the implications of breaches in information security in a number of different cases. In each of these cases, you have asked us to comment on the security breaches from the perspective of our members who operate as nationwide consumer reporting agencies.

I will start with TCI Communications. Our members have no direct relationship with TCI Communications, and we learned—our members report to us that they learned about access codes being compromised in particular through customer contacts with us.

We work collaboratively with our customers. We worked collaboratively then with law enforcement to assist affected consumers. Let me just outline some of those steps.

Consumers received notices from consumer reporting agencies as well as in partnership with our customers to make sure that they were aware of the breach that had occurred with regard to our information. Consumer's files were in some cases frozen temporarily while we could get those notices to them.

Notification letters also then allowed consumers to take advantage of free file disclosures, free access to monitoring services that our members provide, as well as opting those consumers out of prescreened offers of credit, and also adding fraud alerts to their files.

Beyond the priority of assisting consumers, we also took proactive steps to ensure that the scope of the fraud was contained. We analyzed the patterns that we identified through the crime, and we then adjusted our pattern recognition tools and initiated reviews all of all third-party access codes where we had similar third parties having access to those. We began rotating access codes more aggressively. Our customers are more accepting of the rotation of those access codes today.

So we actually have a task force continuing to analyze yet additional steps we can take to further remove access codes from employees who might otherwise take advantage of the access that they have.

We had no real involvement with DPI Merchant Services to the extent that we have been able to ask our members that question.

I will move on to TriWest. With TriWest, TriWest is not a customer, it was not our information involved in this case. TriWest, as they reported themselves, took very quick action. On behalf of TriWest, many consumers then contacted consumer reporting agen-

cies. We provided them voluntarily with free file disclosures. We also took them off a pre-screened offers of credit again, added security alerts to their files.

These are just some of the various initiatives that we have for assisting potential victims or real victims of identity theft. A summary is included with our full comments here for the record.

TriWest then proactively contacted our members and coordinated an additional plan of work that would allow their customers to have an easier time of adding additional information to their files.

We learned a number of things through this experience. One, criminal behavior by employees, we will never be rid of that completely. But, of course, thanks to Mr. Shadegg, we have the Identity Theft Assumption and Deterrence Act of 1998.

Those employees who had access to those systems, in fact, violated that very law that you created in the first place. They also violated the Counterfeit Access Device and Consumer Fraud and Abuse Act of 1984. They violated the Fair Credit Reporting Act, amended in 1996, which also prohibited access and escalated criminal penalties as well as civil fines for perpetrating this type of crime. So we do have a number of different laws on the books today.

That being said, obviously everything that we can do to vet employees who have access to sensitive information is a critical element going forward. We must begin to learn to measure the relative risks of various breaches. One of our concerns from our members is that if we were to encourage the entire Nation with every security breach to contact consumer reporting agencies, this would not be hundreds of thousands, but literally millions of contacts per year.

One of our member companies estimates that it was, in servicing TriWest customers, which was the right thing to do, it was the right time to do it, we have no question about doing it, it cost one of our member companies $1.5 million in order to accomplish that goal.

We obviously need to work with the Congress and work with this issue to make sure that we are not on our own handling the totality of that kind of cost. It would change and radically alter how we do business today.

All of that being said, coordinating assistance for consumers is important, and that is what our initiatives do for victims of identity theft. We look forward to working with you and this committee in this process, doing everything possible for those consumers.

Thank you.

Chairwoman KELLY. I thank you, Mr. Pratt.

[The prepared statement of Stuart Pratt can be found on page 130 in the appendix.]

Chairwoman KELLY. It gives me great pleasure to now call on Mr. John Brady, who is a constituent of mine. And I am very pleased to have him be here to testify from MasterCard today.

Mr. Brady.

**STATEMENT OF JOHN J. BRADY, VICE PRESIDENT, MERCHANT FRAUD CONTROL, MASTERCARD INTERNATIONAL**

Mr. BRADY. Good afternoon, Chairwoman Kelly, Mr. Bachus, Mr. Sanders, Mr. Gutierrez, and members of the subcommittee.

My name is John Brady. I am the Vice President for merchant fraud control for MasterCard International in Purchase, New York.

It is my pleasure to appear before you this afternoon to discuss the important topic of fighting fraud and safeguarding financial information. MasterCard takes its obligations to safeguard financial information and protect consumers extremely seriously. This issue is top priority for MasterCard.

We have a team of experts devoted to working with law enforcement and maintaining the integrity and security of our payment systems. Our success in protecting consumers and preventing fraud is due in part to the constant efforts we undertake to keep our network secure.

The MasterCard Information Security Program is comprehensive, and we continually update it to ensure that it provides strong protections. Our member financial institutions also have information security protections in place, including those required under the applicable banking law.

Also, MasterCard's bylaws and rules require each member and any third party acting on behalf of a member to safeguard the transaction and account information. Our bylaws and rules also require any merchant that accepts a MasterCard branded payment device to prevent unauthorized access to the information.

In addition, MasterCard has a variety of consumer protections and antifraud tools. For example, MasterCard has voluntarily implemented a zero-liability policy with respect to unauthorized use of U.S. issued MasterCard consumer cards. Under this rule, a cardholder victimized by unauthorized use generally will not be liable for any loss at all.

In addition, MasterCard has developed programs to protect against unauthorized use of the MasterCard payment cards. These include enhanced security features on the card, the MasterCard address verification system, and our proprietary fraud reporting system which helps identify fraud at merchant locations and allows us to better focus our global merchant auditing programs.

We also offer a program to our issuers called Risk Finder, which assists issuers in proactively identifying fraud. These and other MasterCard tools have proven extremely effective in protecting cardholders and the security of our systems.

I would now like to discuss a recent example of how we addressed a problem when it occurred. There was a recent incident involving a data processor called DPI, Data Processing International, who was acting as a service provider to a MasterCard member bank in Ohio, which, in turn, was providing bank card processing services for merchants.

Earlier this year DPI detected that someone had obtained unauthorized access to its system. Although it is not clear at this point how much data the hacker successfully exported from DPI's system, we do know the hacker potentially had access to approximately 10 million Visa, Discover, American Express and MasterCard payment card account numbers.

Once DPI detected the problem, they took action, and quickly notified the Secret Service and FBI as well as affected payment card companies. MasterCard immediately took decisive action to protect its systems, its members, and most importantly MasterCard cardholders from fraudulent activity related to this breach.

MasterCard interviewed the appropriate people at DPI in order to determine the nature and scope of the breach. MasterCard gathered the payment card account numbers and forwarded them to the appropriate issuers via our MasterCard alert system.

MasterCard hired a third-party forensic firm to act on MasterCard's behalf during the investigation. MasterCard remains in ongoing contact with issuers of the card numbers that were involved. I am pleased to say that it does not appear that these numbers have been involved with unusual activity as a result of the DPI breach.

As a final point, I would like to note that law enforcement agencies have done a commendable job in investigating this breach. MasterCard works closely with these organizations and greatly appreciates their efforts to resolve this issue.

MasterCard continually strives to provide its members and MasterCard cardholders with strong protections. And we will continue to develop new strategies and tools to prevent those who seek to do harm from succeeding.

I would like to thank the subcommittee for inviting me to discuss these issues, and I would be pleased to answer any questions you may have.

Chairwoman KELLY. Thank you, Mr. Brady.

[The prepared statement of John J. Brady can be found on page 86 in the appendix.]

Chairwoman KELLY. Mr. Hendricks.

**STATEMENT OF EVAN HENDRICKS, EDITOR AND PUBLISHER, "PRIVACY TIMES"**

Mr. HENDRICKS. Thank you, Madam Chairwoman and Mr. Chairman.

A lot of times in the privacy community, we like to talk about Supreme Court Justice Louis Brandeis, who wrote eloquently about the importance of privacy in a civilized society. But, he is also the one who wrote that sunshine is the best disinfectant, and one of the themes throughout my brief talk today is the importance of sunshine, that to improve privacy you need sunshine and transparency. Just by having this hearing today, you are bringing sunshine to a very important issue, and providing a vital public service. I really commend you for that. And again, thanks for the opportunity.

A few fundamental observations. The problem that we are discussing today, of hacker access to sensitive data, data leakages and identity theft in general, is going to get worse before it gets better.

There are several reasons. One, is that we have now in our society many databases filled with the personal data, and they, to me, are the electronic equivalent of swimming pools without fences around them. They are attractive nuisances.

The reason they are attractive is because our personal data is worth a tremendous amount of money to many organizations, and the criminals have figured this out.

The other thing is that identity theft losses are still a fraction of the overall revenue generated by the credit industry. So to this point, the Tower Group has just released a report saying that they don't expect any major changes in the practices of financial institutions because it can still be written off as a cost of doing business.

I don't know if that is going to be very helpful to the people who would be the victims of identity theft, though. In addressing these problems, as I mentioned the lack of transparency is a major issue that comes from all of those cases. Thousands upon thousands of entities, large and small, have instant electronic access to very sensitive data on over 200 million Americans.

Consumers generally don't enjoy that same kind of instant electronic access to their own data. We must move toward a society in which they do, and I will explain why and how.

Also, there is a lack of sunshine when things go wrong, and that is the issue of, are people going to be notified when their security is compromised. Currently there is not a requirement of that.

I will talk about the culture of security that is really needed, and we must develop and advance. Also another problem that comes from all of these cases is the over reliance on the Social Security number.

Now, in the Teledata Communications case, which I think is one of the more important cases we are discussing this morning, you see access as a vital part of the problem and the solution. If those 30,000 victims would have had instant electronic access or alert providing them that there had been activity on their credit report, and one of your constituents from New York or Alabama or Arizona saw there was an inquiry on their credit report from Texas Energy Supply, which is one of the institutions used for fraudulent access, then they would have known something was wrong.

In fact, the credit bureaus have already started offering this service, and they have discovered it is a very good revenue stream. The problem is, they are charging as high as $79 per credit bureau to get a credit monitoring service. If you multiply that by all three credit bureaus, that can run over $200.

It is a good business, if you can collect people's data and sell it back to them at that price. But we should remember that the Fair Credit Reporting Act gives you a right of access to your credit report, and caps how much they can charge for it. Yet, there is no cap for these sort of monitoring services I see moving toward a system where we are plugged into our personal data as being an important part of the solution.

So we should encourage that and see the economies of scale and can make it a win-win for everyone. This is also a model for the financial world. There are going to be databases of sensitive financial information kept by financial institutions that could fall outside the Fair Credit Reporting Act. I think that access is going to be a very important issue to address those problems as well.

Also, I was concerned in this case with the lack of security in the TCI case. Because most of the credit card companies, and Mr. Brady can probably speak a lot about this, have software that mon-

itors our purchases and activities, so they can spot suspicious patterns of activities.

To my experience, I have not seen evidence that the credit bureaus are using this, even though this was a case where there was suspicious activity over and over again.

In the TriWest case, I think one of the most important lessons emerging is the fact that the Social Security number should not be used as an identifier, and really this is a societal problem and a Defense Department problem, that they require that the Social Security number as an identifier, and just proposed a new rule to make it the health identifier for soldiers.

I really fear that we will have soldiers returning from the Gulf War to find that they are victims of identify theft, because of over reliance on the Social Security number. We can explore more of this later in questions if you like.

In the DPI merchant services cases, I think what was most troubling was the secrecy that surrounded the problem. At first they only revealed that there was a hit of credit cards. They wouldn't disclose who—that DPI merchant services was the credit card processor. Then they disclosed that.

DPI told the Detroit News that consumers who were concerned about this should contact their issuing banks. Yet than they declined to name which of the issuing banks were hit. There was no systematic way. Then Visa levied substantial fines in the matter, but wouldn't say who they levied the fines on or for what amount or for what purpose.

So basically, this sort of secret society was saying, "we will make sure that your personal information is corrected, but don't you worry your pretty little head about it."

I think the model for addressing this is California, which has passed a new statute, which takes effect July 1, which basically requires notification of individuals when their information is compromised in these sort of breaches.

What I like about the law is the flexibility it includes, and I mentioned this in my testimony. The notice can be in writing, electronically, in accordance with the Federal E-signature law.

Mr. HENDRICKS. If the cost of notice were to exceed $250,000 or were over 500,000 people, you could do it through a combination of different ways and they list some of the ways you could do it. Whenever you have a privacy problem, reasonableness is the standard for the solution. Any solutions have to be reasonable given the context. It is really case-by-case.

The final thing is that when we have the issues of identity theft, as some of your witnesses have said, the main problem is the problem of cleaning up the polluted credit history. It is time-consuming, energy-consuming and very emotional and distressful. So the idea of having us plug into our credit reports and having a more instant means of communicating with our own data is an important part of the solution.

Thanks.

[The prepared statement of Evan Hendricks can be found on page 105 in the appendix.]

Chairwoman KELLY. Thank you, Mr. Hendricks. I am going to ask you, Mr. Hendricks, a couple of things. Having had my credit

card number stolen, my 95-year-old mother-in-law had her credit cards stolen last week, and she has called me and said I still have my credit card but the bank just called me and said that my credit card number has been stolen and they are going to give me a new credit card. She didn't really understand it. My point is MasterCard called me when my number was stolen. The issuing card company called my mother-in-law, the bank called my mother-in-law. Since this is already being done, I wonder if you have ever estimated the cost of what it would be for banks, people, anybody to have to notify their customers, since there are millions of us.

And after you answer that question I am going to go to Mr. McIntyre and talk to him about his cost. So what do you think that cost is going to be?

Mr. HENDRICKS. I don't know. I have not calculated the cost. I would love to raise the money to do a really authoritative study on that, because I think it is important. But that is why I agree that there are cases where you have—your solution has to be reasonable to the problem. And if you don't see evidence of crime happening then you can find more general ways to try and issue notice. What I don't think is acceptable is that if you have a system where you know there has been a hit of 10 million numbers, if you simply can't even find out which banks—if you are trying to find out if my bank has been hit, you can't find that out, that is a lack of notice I think that is unacceptable.

Chairwoman KELLY. Given the free market one would hope that the banks themselves would do some notification and do that pretty quickly. But you sat there and testified that you felt that the DOD should no longer use Social Security numbers as identifiers. I am wondering—what clicked immediately in my mind is how much is that going to cost?

Mr. HENDRICKS. DOD, I am told by a fairly authoritative source, has a system—because a lot of soldiers do not have Social Security numbers or their dependents in the health care arena might not have Social Security numbers. So they already have a mechanism for generating another random number that can serve that identification purpose. We see this in a lot of other places. You go out there in the Department of Motor Vehicles in the District of Colombia and because of problems they had with Social Security numbers being compromised now for the last few years they will give you a randomly generated number for a driver's license number. If you want your Social Security number to be a driver's license number you have to request it.

So I don't think there is a tremendous amount—in this case the benefits far outweigh the cost, considering how we are seeing these leakages and the rise in identity theft.

Chairwoman KELLY. Well, as a Congressperson we have to be responsible for the way we spend the money. So we need to get some kind of cost estimate.

Mr. McIntyre, I now would like to ask you a question about how much it cost your firm to do the notification that you did. You certainly acted responsively. I think you were a model in the industry to show how rapidly and how proficiently people could access the fact that their information had been stolen. You did a number of things that had to have a bottom line cost. What did it cost?

Mr. MCINTYRE. We had a lot of people cooperating and helping us in that process and we are grateful to all of them, including our colleagues in the Department of Defense. We have spent about a million dollars to date. That is this real hard cost. That is not the cost of having people work around the clock in our company, which we did from the 23rd of December all the way through the 3rd of January. And their impacts to the individuals who were involved in the Defense Department as well. So our real actual financial out-of-pocket cost is now about a million. We are not done with this issue. We cannot take our eyes off this issue nor in my opinion should we take our eyes off this issue until either the perpetrator is caught or we and the Defense Department are collectively convinced and that is no more risk to the consumer from this information being potentially in someone's hands.

Chairwoman KELLY. Mr. Mitnick, what is the single most important step that financial services companies can take to protect large consumer databases? Is there any one thing that you would point out?

Mr. MITNICK. I wouldn't say there is one thing. It is really a mixture of people, security processes and technology, and developing an information security program, because the attacker or the bad guys are going to look for the weakest link in the security chain. If they can exploit physical security weaknesses like with TriWest or potentially technical weaknesses like DPI, the bad guys are going to get the information. And again, I look at the information that is out there like the Social Security number. Anybody with a credit card and access to the Internet can access a variety of online information broker Web sites and obtain anybody's Social Security number. It is out there for sale. So it is really a difficult issue when this information is readily available and this information could be used to apply for extensions of credit.

Chairwoman KELLY. Thank you.

Mr. Brady, I want to know what action you can take against a member bank that violates your safeguards. Have you ever taken action against—well, let me put it this way: Have you taken action against the member bank with regard to the DPI case?

Mr. BRADY. I would be happy to talk to you about the DPI case. I think the DPI case is an illustration of how the system works, how the rules work in this case, such as the immediate notification to us and our ability to protect the consumers by getting the card numbers out there. And I can tell you this: the DPI case with my input is being reviewed by senior management. What I can further tell you is we have some seriously big sticks that we can apply in this case. I think you will see something probably in the next couple of weeks in the public domain with exactly what our position is in the DPI case, what specifics. So I have input into it, but I don't want to go into great detail about it today other than to just let you know that it is being looked at, it has reached the most senior part of MasterCard and that we have definitive rules that can be applied in this case and will be applied.

Chairwoman KELLY. Thank you. My time is up. Mr. Bachus.

Mr. BACHUS. Mr. McIntyre, you mentioned the truncating problem with merchants, people picking up the Social Security number and using that. And just on reading the paper, at least my impres-

sion is that a lot of identity theft and people using people's credit cards is someone at the merchants getting that information off the receipt. And Mr. Mitnick mentioned the fact if you truncate the credit card, you mentioned that too. And first of all, and I am sure—Mr. Brady, could you comment on this—it is my understanding that credit card companies are going to start requiring their merchants to do that in the very near future anyway. So I think that problem will be——

Mr. BRADY. If I could. That is absolutely true. That has been a practice with ATM receipts and receipts when you go to a gas station, truncation for years. But both card associations are moving to that. That will be happening within the next 2 years, so you are absolutely correct. That has already been addressed.

Mr. BACHUS. Can you give us a target date on when that might happen?

Mr. BRADY. I can't give you the exact target date, but I believe it is 2005. But I will confirm that and get back to you on that.

Mr. BACHUS. See if it could be speeded along. Mr. McIntyre, you are talking about truncating and in the situation of a merchant, but let's go back to your situation. Did you truncate the Social Security numbers?

Mr. MCINTYRE. No, sir. Currently we are required to use the Social Security number in its full breadth when we communicate certain information. That is a topic that is under discussion, and I will be making some recommendations to the Department of Defense for the health care system in that area. The important thing to understand, though, is we didn't e-mail the numbers out. They didn't get released on a paper. Someone stole the hard drives. And in doing it in the configuration that they were in at that time it was a database that allowed them to have access to the full Social Security number.

Mr. BACHUS. Aren't there programs where even when they go into your data base it can be programmed to where they can't pull that out?

Mr. MCINTYRE. There is some amazing technology available in the marketplace that I have actually put in place in our organization over the last several months. The fact of the matter is, though, if you go to today's standard it is not good enough 6 months from now. And the challenge in this area is there is so much growth in technology and it is changing so rapidly. Those little Blackberries that we all carry, those weren't available a year ago. It is changing so rapidly that we have got—this is something that you constantly have to stay on top of.

Mr. BACHUS. Let me ask you this. The cost has been mentioned. You spent a million dollars but actually the credit bureaus—Mr. Pratt, I think he represents those companies—didn't they spend about a million and a half a piece? Did you testify to that on TriWest's case?

Mr. PRATT. One of our member companies did run the numbers and spent about a million five.

Mr. BACHUS. Who pays for that if we were to design something and requiring someone to?

Mr. MCINTYRE. I pay for my own cost, which I assume is what that organization is going to do. One of the reasons why they were

willing to move to a process by which we could assist them in filing the fraud flag is to reduce that expense. So we took on that burden, which we willingly do. I don't have any problem with the million dollars I spent. I want to state that very clearly.

Mr. BACHUS. What I am saying, Mr. McIntyre, information was stole from TriWest but it resulted in a million and a half to one of the credit bureaus.

Mr. MCINTYRE. Actually the way it works, sir, when the information is compromised the most effective things the experts tell you that you can do if you have lost the type of information that was stolen from our organization is to get out in front of the issue as a consumer and file——

Mr. BACHUS. I am not arguing with the fact it was done. I am just pointing out——

Mr. MCINTYRE. The only place you can go is to those credit bureaus.

Mr. BACHUS. It was great that they did it. I am just saying other people, as a result of that theft at TriWest, there were other companies that incurred expenses of—actually greater expenses than TriWest or comparable expenses.

Mr. MCINTYRE. No question about that. That is why hopefully when they catch the person we can figure out how to be more creative than just use the maximum 5 years, $250,000 penalty.

Mr. BACHUS. Mr. Hendricks mentioned this. You know, as far as notice in all cases, when you say notice in all cases what if it interferes with a law enforcement investigation? What if the information that you get is not usable? I mean, I guess I am saying when you say notice in all cases, would you like to qualify that?

Mr. MCINTYRE. One has to be very careful about under what situations you are deciding to provide notice. Where you end up in a case where the experts would tell you there is sufficient information to misuse it and obtain credit, that certainly is an area where you need to do notice. That is what happened in our case and what has happened in a series of cases.

Mr. BACHUS. I understand that. So actually notice in all cases really is notice in all cases where it would be reasonable to assume?

Mr. MCINTYRE. Absolutely.

Mr. BACHUS. Not actually in a case where the information wasn't usable or there wouldn't be any reason to notify?

Mr. MCINTYRE. And I think that California's standard is one that is worthy of looking at. They do talk about reasonable notice, reasonable timeliness under reasonable circumstances.

Mr. BACHUS. That is what—and rush to notify in all cases. I think, you know, there are times when it is not reasonable.

Mr. MCINTYRE. Agreed.

Mr. HENDRICKS. May I comment on that? First, you have a reasonableness standard. I think my point is that the default should be that there should be notice. The general rule should be the notice and you have to justify when and why there will not be a notice. What is also important here as we talk about costs is look at the costs we have identified already just from the lax security procedures, what the credit bureaus had to spend to give people this rush of access to their credit reports, to the notice that TriWest had

to do to notify a million people. Please don't forget the cost to the individuals that then have to spend time and emotional energy working on that. These are very costly matters if we don't get them right.

Mr. BACHUS. If you all would like to respond. Do you have any comment on that?

Mr. PRATT. Well, in terms of the broader discussion, we agree that, first of all, not every security breach ends up in large scale, for example, identity theft. Doesn't mean that some don't. An example is in California 200,000 state employees' records were ostensibly or allegedly stolen. Our member companies cooperated with that breach as well. So there are 200,000, there is 562,000 and the risk potentially of 10 million over here. So you can see where the concern rests.

We have tracked the 200,000 out of California and have not had a single incidence of identity theft related to that. Now does that mean we should do nothing? Of course not. But there is a lot of qualification that has to be gone through and deliberative process that we have to work our way through to make sure we are doing the right decision at the right time. In all of this obviously our members believe that if we have had our information breached it is a responsibility we have to take seriously, not just under fair credit but it is the right steps at the right time for the consumer, and, no differently than any other industry represented here at the table, we are going to take the right steps for the consumer.

Mr. BACHUS. I think you are in the better position in most cases than people who don't have all the facts.

Mr. Brady, would you like to respond?

Mr. BRADY. I guess I would like to respond specifically to DPI and how it relates to this, because I think what you have to understand in the DPI case is that there has not been fraud on those accounts. And we notified the issuing banks promptly of the issue and the issuing banks in turn may notify their cardholders; in some cases they notified their cardholders. But the message I want to send here is one of let's not create panic here. You will read the headlines that something bad happened but the by-line on page 6 is that something good happened. And yes, something bad happened at DPI. But the message is that a lot of good things happen. There are a lot of people behind the scenes protecting the integrity of the process.

Mr. BACHUS. I think by talking about them to a certain extent allows people to—you know, Mr. McIntyre was telling me that happened to him, actually happened. There was a bank that had something very similar. Had he had notice of that, he probably could have avoided this entire incident. So I believe by highlighting this and taking steps that we are already preventing a lot of that and some of the proposals on the table.

Mr. MITNICK. I have to ask a question of why would these companies not encrypt the credit card and financial information that is in their databases. Because if the bad guys are able to break into these systems the information is unintelligible. So maybe that is a standard that should be considered in the industry.

Mr. BACHUS. Certainly if that happens notifying people would actually—I think that would be a downside. That would be something you wouldn't want to do.

Chairwoman KELLY. Mr. Mitnick, what would that cost?

Mr. MITNICK. What would the notification cost or the encryption? Well, there are different cost factors. If you encrypt stored information it is relatively inexpensive. If you are encrypting data in real time it is expensive. The actual dollars and cents I don't have at my fingertips at the moment.

Mr. PRATT. I can attest to that. We operate as an association information exchange at financial institutions. When we have to hire three different terms to management in description process and testing on a monthly basis for penetration, it is staff, it is outside resources, it is internalized resources, it is software programs. I think Mr. McIntyre said it just right in every 6 months you have to change everything because you have to ramp up to a whole new standard because the criminals are moving almost with you and keeping pace in a lot of cases.

Mr. MITNICK. Not necessarily with the encryption as long as you are using an algorithm that has been widely accepted and you are changing keys on a frequent basis. So that is my comment for now. I had something, but it slipped my mind, that I was going to say.

Chairwoman KELLY. Mr. Shadegg.

Mr. SHADEGG. Thank you. Let me begin, Mr. McIntyre, with you. Your testimony doesn't go into great detail about the break-in. I think it might be helpful if we heard a little bit more about how it was accomplished, how you discovered it.

Mr. MCINTYRE. Yes, sir. I will be as detailed as I can be given the fact that it is still under Federal investigation with the FBI, the Defense Criminal Investigative Service, and a number of other entities, and hopefully they will crack it soon. But we suffered a theft following another theft, and what happened on this particular Saturday at a building where we have no signage on the doors on the building that we are there is that someone broke into the property management office for that site and stole the master electronic key in order to enter our suite. Totally undetected. Many of the offices around here have those proxy cards. It allows you to know who is going in and who is going out, what time they go in, what time they go out, and their identity. And so it was a fairly sophisticated job. Was it an insider job? We don't know. The authorities don't know. They visited with 150 different people. They polygraphed a lot of folks. They have caught other people who have been engaged in other similar crimes, but not ours in the process of this investigation. And we have a very serious problem in Arizona as it relates to this issue, as you well know.

Mr. SHADEGG. It has already been brought out in your initial testimony and questioning that you were required to maintain Social Security number information for these customers.

Mr. MCINTYRE. Correct.

Mr. SHADEGG. It seems to me and, as you know, I have put a lot of time into the health care industry, are we disadvantaged, are we doing ourselves a disservice to require a single number like that and to have—and to, for example, require you to use it? I take it you use the Social Security number because of a DOD reg and

DOD is using Social Security numbers by choice, presumably not by statute?

Mr. MCINTYRE. Forty years ago they used to use an ID number and they switched to Social Security numbers. I am not an expert in why they switched and what the complications were that led to that. Probably somewhat trying to remember what all your different numbers are because I can't remember my pin number if I have been up all night. So there are different issues that would lead one to do that. My Blue Cross/Blue Shield card that I carry in my wallet has my Social Security number on it. So this is something that we all—I think you all need to take a look at. Where is that really necessary and what are the complications if you are going to move away from that? We are required to use them in our current contract.

Mr. SHADEGG. To that point I would like to ask any member of the panel that wants to make a comment. Do you think numbers should be further restricted, the use of Social Security numbers, and should the DOD be using a different number than their Social Security? When I was on active duty in the military they used four digits of my Social Security number and it seems to me it is too broadly used. Anybody have a comment?

Mr. HENDRICKS. I would like to comment on that because I think, yes, pending a study of the costs, the actual real costs, they won't be hard to calculate, I think we should basically place a moratorium on further use of Social Security numbers. It is already required by banks and employers and we have passed laws and we have this. But it is such an instrument of choice by identity thieves and it increases the value of information and the incentive for stealing it. So I think that we should look toward having—especially in the health care field it is very problematic that the Social Security number is used.

The last thing you should remember is you didn't have time to fit the most recent case onto your agenda. That is the University of Texas, who got hit by an outside hacker. He was hitting their system with random Social Security numbers and once he found one it would suck it out of the system and was able to get thousands and thousands of Social Security numbers through this program. The University of Texas official said this was a mistake. We should not have used the Social Security number. We are changing. So I think we should do this more systematically instead of lost and found, by trial and error.

Mr. SHADEGG. You said pending a study of cost. It looks to me there are costs everywhere here. We will have cost to notify everybody. Mr. McIntyre recommended that there should be an obligation to notify everybody. I think that ought to be universally true. But that is expensive. Mr. Mitnick commented about encryption and then we discovered you can encrypt stored data but not current data. It is the current data that is at least viable. So it seems to me we are going to face costs to secure these systems no matter what. Go ahead.

Mr. PRATT. I thought I would set this into context a little bit. We do have a difficult time in our society today with 40 million consumers moving every year, 3 million last names change due to marriage and divorce, about 6 million or 7 million second homes in

this country with a lot of folks who move in between those two homes. There is a lot of flux in the ways we think about identifying ourselves. When you and I think about ourselves and we look at our own mail coming in the door, we go I know who I am and I know what my information is. For a database like a consumer credit reporting database which must have reasonable procedures to assure maximum possible accuracy of the information in the file, that is what the Fair Credit Reporting Act tells us, it would be very hard for to us build an accurate database if we did not have the Social Security number at least for those internal accuracy purposes.

I think one of the issues that we haven't framed the question quite this way is access by the general public to Social Security numbers different than the use of the Social Security number in certain matching processes internalized, which allows us to build more accurate databases.

Mr. SHADEGG. Mr. Mitnick.

Mr. MITNICK. It is fine to use a Social Security number, but not to authenticate the person's identity. I think that is where the mistake is being made. I know it is a very expensive proposition, but the problem is people's Social Security numbers are readily available. There is—for example, the U.S. courts have PACER, public access court electronic records, and anybody that has had a bankruptcy, anyone could subscribe to the service and look at the party's Social Security numbers. They are there for anybody's viewing. Social Security numbers are easily obtainable and to use them as a means of identification I think is a mistake.

Mr. SHADEGG. Speaking of the government's complicity in this, Mr. McIntyre, isn't one of the cases that you have in this summary the result of the United States Senate publishing Social Security numbers?

Mr. MCINTYRE. Yes, sir. I learned from a number of our Nation's distinguished general officers that they received training when they become a general officer on identity theft, and they receive that because there was a practice up until the late 1990s when on their confirmation in the Congressional Record their Social Security number and name was printed. Someone went out, published that on the Internet, it was taken, they ordered credit and abused the credit of those general officers. The striking thing to me was that criminal got only 2 years and 9 months for that crime. And it takes longer for those people to clean up their credit records than it did for the penalty that the criminal got.

Mr. MITNICK. One other case, I believe it was a New York busboy had obtained the personal identifying information of celebrities that were like the top 100 and started obtaining their identity credentials and applying for credit. That was a huge case out of New York that you might not be aware of.

Mr. PRATT. If I could add one point, I have heard Mr. McIntyre say several times it takes longer for people to clear up their credit history than it does for the perpetrator to remain in jail. I appreciate his enthusiasm for quoting some of the consumer groups in terms of that statistic. We are processing consumers every day successfully through consumer dispute processes. We recently looked at 5,000 credit reports where security alerts have been added to see

if additional activity occurred in those files. In one-half of 1 percent of the cases was there ever even a subsequent dispute relative to that set of 5,000 cases where we had added security alerts to the files.

I have to resist the characterization of our entire industry of being slipshod and unable to keep information out of the file and unable to be responsive. What is happening, and this is why in our initiatives that you will see in our testimony, it is a longitudinal crime. It isn't like burglary. It is over a period of time. So in some cases we are able to correct the initial information in the file but there is still crime occurring or there is still more bad information on its way to the credit bureau file.

So understandably from the consumer's perspective, that is all the same thing to me. But from our perspective we are wrestling with trying to keep the right information in the file for safety and soundness purposes, which is of course important to this committee, and at the same time to keep the fraudulent information out of the file, which is something that we believe is a top priority job, one for us just as it would be for anybody else.

Mr. SHADEGG. In defense of Mr. McIntyre and those consumer groups, I can tell you that my constituents who brought the first legislation to me they spent far longer than 2 years and 9 months trying to clean their record up, indeed probably four or five times that length of time.

I guess the problem I have is the reality that both summaries are wrong and really the real problem is how long it takes to apprehend them, because in most cases they are not apprehended at all.

Before the earlier act passed the response of law enforcement—and I know this is not your responsibility—the response of law enforcement was to say this isn't a crime. They may have stolen your identity but until they use the credit and you can show me the credit then I have a credit card fraud case. And, by the way, I am only interested in that credit fraud case if you live here and the credit card was used here. If the credit card was used in Pennsylvania and you live in Phoenix, Arizona, I don't care. So we have a serious problem we have to address here.

I want to conclude by asking Mr. McIntyre if you would describe how the fraud alert security mechanism works and what changes or improvements would you suggest making to it?

Mr. MCINTYRE. I am very grateful to the credit bureau industry for what they have done. I am sorry that my remarks were misinterpreted, because I actually think that the Federal laws need to be enhanced and the penalties. I think the bureaus have done a good job of helping protect consumers wherein they have been notified and they are aware they can get that protection.

What I was advised to do was to contact the consumers, let them know this had happened. Because the most effective thing you can do when this occurs and you have information in the public domain that could potentially be used to create credit and misuse it is to put a fraud flag on your file. What that does is it notifies those that may be interested in granting you credit or may be contacted to grant you credit that they need to verify you are who you say you are so your identity isn't misused and you end up with a subsequent problem. That is why we took that action. We were advised

by the bureaus and the FTC that was the best thing to do in this case.

What I have discovered, together with the bureaus, is that we do need a process by which corporations that are willing to do this on behalf of their customers can do it. It helps the bureaus reduce cost and it helps the customer reduce the hassle, because it was on average taking 3 hours for people to go through this process just because of the sheer weight of the volume that had been put onto the back of the credit bureaus.

The second thing I discovered is that in order to keep people protected I now have to notify people every 90 days that they have to go out and update their fraud flag because each of the credit bureaus is on a different cycle. One of the credit bureaus requires an update every 90 days. One of the credits bureaus requires an update every 6 months. One of the credit bureaus requires an update everybody 12 months. I think it would be helpful for them and for us and for the customers to have that in alignment.

The issue I face now is when I update people in the next 4 weeks that unless the crime has been solved, and I will update them about that, but their information is potentially still at risk. Guess what, some of my customers are now deployed. Their fraud flags could drop if I don't make sure and the credit bureaus together with me don't make sure that stuff stays. So we are talking to the credit bureaus now and we are going to talk to the Defense Department and the lawyers to figure out how do we get around that problem.

Mr. PRATT. In fact, every one of those consumers when they contacted the credit bureau can add a 7-year alert to their file. So that once you contact the bureau what we are talking about is two different things. The temporary alert is added by the credit bureau without a question. In other words, the consumer said I want you to believe me at least to a certain extent, I don't have to go through a bureaucracy just to get a fraud flag on the file. The key here is once the consumer receives his or her file disclosure and goes over the report at that time a 7-year alert can be added to the file and our member companies are consistent across the board in adding 7-year alerts. So I think there is a difference in practice, or at least we need to clarify the practice here.

Mr. MCINTYRE. I would suggest in cases where the crime may actually be solved because there is lots of focus of law enforcement on it that the hassle of having a long-term alert may not necessarily be the right action. But I am not an expert in this area.

Mr. PRATT. Of course after a consumer discovers that he or she is safe we will voluntarily remove that alert any time during the 7-ear period.

Mr. SHADEGG. I know I have more questions, but my time has long since expired. I will yield back. If there is a second round, I will take advantage of it.

Chairwoman KELLY. Mr. Renzi.

Mr. RENZI. Thank you, Madam Chair. Appreciate your testimony and traveling all the way out here, especially from Arizona, and sharing with us the sophistication behind the theft operation and particularly that struck TriWest. Many of you know, particularly my friend from Arizona, I am the father of 12 children, 7 boys and

5 girls. I am particularly concerned about the niche as it relates to how we take care of the children's identity that has been stolen. If the identity of the parents had been stolen, name, address, phone numbers, everything, then obviously also the child's address. We go back to the days of those spy movies where they would take identity theft out of the obituaries. We now move forward into electronic theft, full and complete information provided not just on adults but on children. You can imagine a child of 5 or 6, 7 years old having their identity stolen from them and then yet no flags go up until they are about 18 years old, 16 years old and all of a sudden for the last 10 years their identity has been stolen, their identity has been used.

So I would ask what kind of remedies, and I know there is some talk in this area, what kind of remedies are you looking at, what kind of means are we putting together to help protect our children?

Mr. MCINTYRE. I can't respond to that part of the question, but what I can tell you is we did many responses to that issue. We looked at that. We were concerned about that issue. I have three young kids, so it is the question of what impact is this going to have on them. The fact of the matter is that in our case all of the information, the breadth of it, on the people over 18 was not also on the database for the people under 18. In some cases it was just their name. In other cases there wasn't any information because they were—the primary sponsor was the one who was actually on the database.

What we did was we talked to the FTC, we talked to the credit bureaus, we talked to others who were experts in the industry what do you do, how do you deal with this issue? What we did was set up a database. The database can be reviewed by the primary sponsor to determine what information was on the stolen hard drives to determine what secondary impact it may have on them or their families and then to advise them of the risks if you add a fraud flag for kids under 18 who have no credit record, and then how you would go about doing that so that they could make an informed decision on their own, and then we have offered to assist them in that way.

Mr. HENDRICKS. I would like to respond to that because I am working with some folks on a case right now where a young man from Alabama was mixed up with an older person from Arizona actually. Just an old-fashioned mixed file case based on a similarity in Social Security numbers. They weren't the same but because the algorithms, if they are just one or two digits different they will merge the files. What is troubling in the case is the young man from Alabama is basically being assigned unpaid debts from when he was like 12, 13 and 14 years old. So you would think the system would identify that at his age he wouldn't have been able to incur those debts. But they don't seem to have a system in place. He has had a terrible time getting his files unmixed. His mother has gotten involved. So when he became of age and his rite of passage, when he got to apply for credit he was rejected. So there are some very old-fashioned problems in this system.

Mr. MITNICK. In certain States like California, Texas and Kentucky birth records are public record. You can go onto the Internet and look up anyone's birth record which gives criminals the ability

to apply for that person's birth record because all they need to do is send a letter to the Department of Vital Statistics, give them the information on the birth certificate, they get a certified copy of the birth certificate back, and they become that child. They can get extensions of credit set up and the account at the credit bureau. So that is a problem that certain States have, birth records in the public domain.

Mr. RENZI. Thank you. One of the things I know that is being kicked around as a remedy is the idea—Mr. McIntyre, I appreciate you mentioning it—is that those children who have had their identities stolen from them would have an alert or flag put on their credit. So that if anyone was checking their credit, if anyone was using their credit, even when that credit was being checked it would warn the person checking the credit that, hey, this is a stolen identity. Let's say a child goes through 10 years of that and then all of a sudden it is time for them to use their credit. What I worry about on the alert system is how do you then take it off? What detail is provided to show that child was innocent. So as we look at remedies we also not only impose the remedy to protect the child but then the release in order to have the child given back.

Mr. McIntyre.

Mr. MCINTYRE. That is exactly why I felt uncomfortable making the decision to advise people on what they ought to do and that it made more sense to lay out the facts so that every parent who might otherwise have someone on that list could look at the information that was there and make an informed decision on their own, and each parent needs to do that.

Mr. HENDRICKS. I agree this fraud alert is kind of a sledgehammer. It is sort of all or nothing. And I think what is common if have you a problem, you say we don't want my information used for pre-screened offers, too. So you wipe yourself from all those. Obviously we need a finer tuned system so you can really sort of go in with the scalpel and fix problems. But that is what we have now. To me that is why it is very important to have instant access to your credit report so you can see what is on it and what activity has there been on it. That is the best way you can keep it accurate.

Mr. MITNICK. How about developing a partnership with the Social Security Administration so these companies could determine the age of the person requesting the extension of credit, verify that the name really did match the Social Security number, because it would be kind of strange for a 16-year-old to be applying for a MasterCard.

Mr. RENZI. Well said. Creative idea. I serve on the Veterans' Affairs Committee. At this point in our Nation's history we have got women with children, men with children in America who are being kicked out of their homes because the checks, their military pay doesn't get home in time. And we are looking at legislation that is going to protect our veterans and servicemen and women so that you can't move them out of their dwellings, you can't take away their cars if they are late on a payment. I am thinking how this might tie in this piece of legislation that we are working on in that if a serviceman or woman was to have their identity stolen, and since we are barely paying them enough anyway, the cost for them to get their identification back is going to be enormous. And that

cost or that loss of revenues could then impact their ability to house their family, to provide decent transportation.

Is there an ability or would you be in agreement, particularly Mr. McIntyre given the fact that you helped the TRICARE portion and how it affects our servicemen and women, would there be an ability to protect our servicemen and women as it relates to identity theft?

Mr. MCINTYRE. I would be more than willing to look at that with you. You have described exactly why I have no qualms nor does my board to spent the kind of money and effort that we have had to spend. The thing that concerned me greatly about the case that involves us and the theft that was perpetrated against us and the information involved is because we are talking about people who serve all of us who do not make a lot of money and a blight on their credit report can be the difference between having a car, renting an apartment or buying a house. And so we felt an absolute obligation to do what we did. But I would be glad to work with you, sir, in that area.

Chairwoman KELLY. Thank you very much. We have just been called for another vote. In the interest of time I am going to call on Mr. Moore and I am going to call on Mr. Fossella. I would like everybody to keep their questions and answers within the 5-minute period, please.

Mr. MOORE. Thank you, Madam Chairman. I wanted to just ask you a couple of questions, Mr. McIntyre. We have talked before and I appreciate the actions that your company has taken since the theft, the burglary and the theft to try to—and your personal call to the people but I wanted to ask, obviously I think it is in everybody's best interest that not only do we punish somebody who has committed a crime like this but we try to prevent it in the future and that is the best way to protect people, I think. I was concerned in reading some of the materials, I think in your State, that I think it was 2 days after the incident until you even learned that there had been a theft.

What kind of security precautions did you have or security systems did you have in place on the day of the incident? And apparently they failed.

Mr. MCINTYRE. I have been asked by authorities not to address all the details of the security systems and the like because they are still attempting to catch who did it, and FBI agents have interviewed over 150 folks and polygraphed a number in this area. What I can tell you is that we were the subject of a secondary theft. Whoever was responsible for this broke into the property management office, the place where we had this secondary office. They then stole the electronic master key which allows you to get into a locked door undetected, although it would read as though you were the property manager, and enter our suite. And that is how the theft occurred. Thus we weren't aware—it happened on a Saturday. We didn't learn about it until first thing Monday morning when our folks when in to turn on the computer and found out that the computer system did not work.

Mr. MOORE. Obviously there are video monitor systems and security systems and other precautions that can be taken to notify somebody if there has been an entry even if it appears to be an au-

thorized entry, because at some point they had to steel the electronic key, isn't that correct?

Mr. MCINTYRE. Correct.

Mr. MOORE. From your materials in your statement it appears that you have and I hope that you are taking substantial strides in trying to correct the system so something like that doesn't happen again. If there is an unauthorized entry, you or somebody would be notified immediately.

Mr. MCINTYRE. I will tell you that we have brought in security experts, we have partnered with the Department of Defense. They are now looking at their entire system worldwide. They found deficiencies in their areas. But you know what is interesting to me about this is that in Arizona 6 months prior to the theft in our building, five financial institutions were hit with a very similar crime. A bank in Tucson was hit 6 months prior after hours. Penetrated all the security systems, got through, stole the hard drives, left the bank with that information. And so this is something that unfortunately, given the rise of the prevalence of information and the like, that we have a real serious problem with in this country. That is why I think when it does happen, even if they are able to get beyond the safeguards, that is when we have to look at where are the responsibilities for notification.

Mr. MOORE. Absolutely. How long after the incident was it that you notified the Department of Defense?

Mr. MCINTYRE. I notified the Department of Defense immediately when I discovered there was a problem. They then ran the database and we contacted the senior management in the Department of Defense, not the operations people who we had contacted the first day that we discovered it. We contacted them once we had the database fully run and knew what the extent of the problem was.

Mr. MOORE. Thank you. I will conclude by saying when these large databases exist and if in fact hard drives are stolen, not just data or information from a computer system but hard drives and there has to be a physical entry and I hope that you have told me and I trust what you have said that your company is looking at this very seriously and making sure this doesn't happen in the future. I think financial institutions, anybody else who has databases like this needs to take similar precautions.

Chairwoman KELLY. Mr. Fossella.

Mr. FOSSELLA. Thank you. I will just throw out two questions and the second is sort of two parts and allow you to answer in light of the time here.

First, Mr. Brady, in light of your efforts at MasterCard I am sure you are doing what you think is providing the highest level of security on the network. In your mind—if it has been asked before I apologize—in your opinion what would be the best thing that could be done to provide incentives perhaps for other companies to do as you are doing and in providing the highest level of security? And secondly, I will throw this out to all of you. If you can answer me, great.

Earlier the Secret Service testified and argued, it seems, for a better working relationship or continued working relationship among different agencies and academic institutions to prevent what has been alluded to a number of times here. In your experi-

ences how have those relationships been working and what, if any, ways can those be improved? And the second part of that question is the cost of prosecution and whether local or State or Federal prosecutors are doing what they can given the resources they have.

I will give you an example. It has been argued that perhaps a local district attorney, given the nature of this type of crime, will say, hey, I have a limited budget here; in my view, the cost of following through on prosecution to indict with a conviction is going to cost me X amount of dollars, which could be, you know, such a disproportionate share of my budget that I don't have those resources to follow through. So are there any ways to, A, if in your experience that is true, and, B, if so, are there any ways in which those situations could be addressed in order to prosecute those crimes as efficiently and as swiftly as possible?

Mr. BRADY. Yes. I would like briefly to talk on your point of security. MasterCard, without getting into too much data on our security network, has a very robust network. We do outside penetration testing on networks to ensure they are secure and they are. One of the things that I really want today to bring out here, and I alluded to it before, was there is no need for hysteria because MasterCard is vigilant behind the scenes. When there is a compromise and the DPI hack is one of those examples, We notify the issuers, we follow the protocol, we not only follow the protocol of MasterCard and working with law enforcement, but the entity that was breached follows the MasterCard protocol in place, the timely notification to us and also the timely notification to law enforcement. We have sufficient penalties in place so that if that didn't happen that they could be fined on a per day basis, a draconian amount of money.

So I think the law enforcement gentleman brought up that these companies are coming forward, and part of that is because there are effective rules in place to bring them forward when something does happen. And the good news again with the DPI hack is we are not seeing general fraud. But everybody is being vigilant, looking at the account numbers, and monitoring the account numbers on a daily basis.

And MasterCard has a wide array of fraud controls in place, I know we are short on time, but we have controls in place for auditing merchants, controlling fraud, and we have penalties and policies in place for the bad actors that are in the system.

So your second point was on law enforcement and our relationships, and from where I sit we greatly value those relationships. The gentleman from the Secret Service that were here from this morning, the electronic crimes task forces that have been put together over the past several years, the effort is tremendous and it really fits a need out there. And I would just like to say that one thing that was brought up this morning about these hacks and what we find out from the hacks is that there is little fraud on the hacks. When you see account numbers that are being hacked we track it. There is little fraud on it. And you know what it is? A lot of them that are out there that are joy riding, that are stealing numbers, that are causing harm. And the question is what do we and the prosecutors that are out there, do with them not only in the Federal level but the State levels. I will wrap up. Sorry. And

I think tougher penalties are important here because even though there is not fraud there is a lot of costs when these things happen.

Chairwoman KELLY. Thank you very much. The Chair notes that some members may have additional questions for the panel. They may wish to submit those in writing. Without objection, the hearing record will remain open for 30 days for members to submit written questions to the witnesses.

The second panel is excused with the committee's great appreciation for your time. Thank you. I want to thank all the members and staff for their assistance in making the hearing possible.

This hearing is adjourned.

[Whereupon, at 1:25 p.m., the joint subcommittee was adjourned.]

# A P P E N D I X

April 3, 2003

**OPENING STATEMENT OF CHAIRMAN SPENCER BACHUS**
**"FIGHTING FRAUD: IMPROVING INFORMATION SECURITY"**
**APRIL 3, 2003**

Thank you, Chairwoman Kelly, for convening this joint hearing of our two subcommittees to review issues related to the security of personal information. This is an issue of critical importance to the financial services industry, and I believe this hearing is a timely one. This hearing, which is titled "Fighting Fraud: Improving Information Security" is one of many hearings that will be held by the Subcommittee on Financial Institutions and Consumer Credit regarding the security of personal information. I expect that at some point our efforts will culminate in comprehensive legislation addressing the broad issue of how secure consumers feel with respect to their personal information.

Today's hearing will focus on three cases where sensitive personal information was compromised through hacking or physical theft of computer databases. Each case that we will hear about today is illustrative of a different type of security breach – an outside computer hacker, employee misconduct and a garden variety burglary. Using these cases, we will review how credit issuers, third-party vendors that process transactions, credit bureaus, and law enforcement coordinate efforts to limit harm to consumers when data security is breached.

Fighting fraud and protecting the security of personal information is a topic that unites financial institutions and consumers: each group is harmed by the fraudulent use of personal information. Financial institutions are the victims of fraud because the financial institution is usually liable for any losses suffered as a result of the fraud. Consumers obviously suffer unnecessary inconvenience and insecurity as a result of fraud, and they can be exposed to additional crimes such as identity theft. Furthermore, at least a portion of financial institutions' fraud losses can be expected to be passed on to consumers in the form of higher prices. There can be no doubt that when fraud is committed, everyone loses.

For obvious reasons, financial institutions take precautions to prevent fraud, including precautions to protect the security of personal information. In addition to the self interest financial institutions have in minimizing their fraud losses, Congress has required financial institutions to maintain appropriate standards relating to information security, including standards to protect against unauthorized access to a financial institution's customer records, as part of the Gramm-Leach-Bliley Act. The requirements, as adopted by the federal banking agencies, also require financial institutions to oversee their relationships with third party service providers, including having the service providers agree by contract to implement a comparable information security program. It is my understanding that the federal banking agencies have been examining financial institutions with respect to their compliance with these requirements. However, I remain interested in learning more about the role service providers play with respect to information practices, and their ability to maintain appropriate information security programs. It is my understanding that the Bank Service Company Act gives the banking regulators broad authority to examine third-party providers. Two of the cases today illustrate that greater oversight of these entities may be necessary.

As part of the Gramm-Leach-Bliley Act, Congress also enacted stiff prohibitions against a practice known as "pretext calling," which is a fraudulent means of obtaining an individual's personal information. Pretext callers contact a financial institution's

employees and attempt to obtain customer information, usually while posing as the customer whose information they are trying to collect. This is a serious issue, and one which this committee has held several hearings previously. I am interested in learning more about efforts to enforce this prohibition and the Federal Trade Commission's views on the amount of resources devoted to fighting this fraudulent practice.

[Congress has not been the only interested governmental party with respect to information security and fraud prevention. The banking agencies have also taken proactive steps to ensure that consumers and financial institutions are protected against fraudulent and criminal activity. For example, in order to assist financial institutions in adopting the appropriate security measures, the banking agencies have jointly issued exam guidance with respect to their information security guidelines. The banking agencies have also jointly issued guidance with respect to customer authentication in an electronic banking environment. The Comptroller of the Currency has also issued bulletins or advisory letters on managing risks that may arise from business relationships with third parties, on identity theft and pretext calling, and on network security issues.]

We will also hear this morning from federal law enforcement agencies about their approach to countering those who would compromise the security of personal information. It has always been my experience that law enforcement and the financial services industry work well together with respect to pursuing those who attempt to commit crimes against consumers and financial institutions. I look forward to hearing about law enforcement's perspective on this important topic, especially with respect to whether the representatives from the FBI, Secret Service, and FTC believe they have been given the proper resources to investigate financial crimes.

In short, financial institutions, Congress, the federal banking agencies, and law enforcement have been working to address information security and fraud prevention issues. Regardless of the great pains taken by all of these parties to protect the security of personal information, the chance remains that a breach may occur. Therefore, Congress must remain vigilant to ensure that existing requirements are implemented appropriately and examine whether new safeguards are necessary. Furthermore, it is just as important for financial institutions to have mitigation plans in place in the event that their information security program is hacked or otherwise compromised. I am pleased that we will hear from several witnesses today who will describe how various parties took action to address recent data security breaches and prevent subsequent fraud.

Before we proceed, I believe that it is important to mention that although this hearing is a public forum, we should avoid discussing specific details which may give criminals ideas, or even a roadmap, for doing further harm.

Let me close by thanking Chairman Oxley for recognizing the importance of improving the security of personal information and scheduling this hearing. We must continue to work to improve security and protect sensitive data to ensure that consumers continue to have confidence in our nationwide credit system as well as our financial services system in general. I look forward to working with the Chairman, Mrs. Kelly, and my other colleagues as we continue to examine this complicated issue.

I yield back the balance of my time.

**OPENING STATEMENT OF REP. SUE KELLY**

**CHAIRWOMAN**

**SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS**

**"Fighting Fraud: Improving Information Security"**

**April 3, 2003**

Personal information must be safeguarded throughout our national credit system. Just as consumers shred their unwanted mail and take care with their receipts, financial institutions must develop and upgrade their information security procedures to protect consumers.

Financial records such as credit card numbers, combined with other pieces of personal information, are the first targets of identity thieves. Years of work are often necessary from both consumer and business victims to correct damaged credit histories and restore access to credit.

Today two Subcommittees will hear from witnesses on three specific case studies to review current industry practices and to ensure that proper security procedures and protocols are in place or are being implemented:

> Teledata Communications is a company in my home state of New York that enables businesses to access credit bureau information so they can grant credit to consumers. An employee inside the company allegedly stole and sold passwords and codes for accessing credit reports for thousands of people. According to law enforcement, his actions resulted in millions of dollars of financial theft.
>
> TriWest Healthcare, an important healthcare provider for our active duty military personnel, honored veterans, and their dependents, suffered the physical theft of its computer hardware. The equipment stored personal information about many heroes now involved in the war to liberate Iraq, including the Chairman of the Joint Chiefs of Staff, General Richard Myers. Fortunately, quick action by the company and the credit bureaus appears, thus far, to have prevented misuse of the information.
>
> Another company, Data Processing International in Nebraska, saw its database of millions of credit card numbers hacked from the outside. It again appears that rapid action, this time by the company and the credit card companies, has prevented improper use of the numbers to date.

Through the examination of these cases, the Subcommittee will review how credit issuers, third-party vendors that process transactions, credit bureaus, and law enforcement agencies coordinate efforts to limit harm to consumers when data security is breached. Among our witnesses are officials of the law enforcement and regulatory agencies involved with these and other such cases; representatives of the companies involved; one of the most famous computer hackers in the world, now a consultant; and an expert in privacy.

I want to thank my distinguished colleague, Representative Spencer Bachus, the Chairman of the Subcommittee on Financial Institutions and Consumer Credit, for joining with me to hold this important joint hearing of our subcommittees. I also want to congratulate him for his leadership in the bipartisan passage of H.R. 522, the "Federal Deposit Insurance Reform Act of 2003," by the full House yesterday.

**Opening Statement**
**Michael G. Oxley**

**Subcommittee on Oversight and Investigations and the Subcommittee on Financial Institutions**
**"Fighting Fraud: Improving Information Security"**

**April 3, 2003**

---

This February, a computer hacker broke into an information processor's system and accessed the credit card numbers of over 11 million Americans. In December, a group of thieves stole computer systems containing detailed health accounts of over half a million military veterans and dependents. In a third recent case, an employee of a major software company stole countless numbers of consumer credit reports, ruining the credit of over 30,000 people.

That's tens of millions of Americans being put at risk in just the last year alone. And when your information is stolen, it can take months, sometimes years, to fix all the records and restore your good name.

Information thefts are also hurting American businesses. Cyberthefts are costing American businesses over $400 million annually, in addition to countless more spent on preventing unauthorized access to sensitive information, and mitigating damage to consumers. By many estimates, information theft is one of our fastest growing crimes, more than doubling over the last two years.

In 1999, I sponsored a provision that became law, requiring all businesses significantly engaged in providing financial products or services to consumers to ensure the security and confidentiality of sensitive information. My provision also required our government agencies to "establish appropriate standards relating to administrative, technical, and physical safeguards – (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

This provision has only recently begun to be implemented, but it is clear that we need to continually examine the issue. Information sharing is a critical part of our economy. But consumers will quickly lose confidence in our nationwide credit system if we don't do everything practical to improve security and protect sensitive data.

This hearing will help us determine, at least in these three cases, what went wrong, what has been fixed, and whether there are any larger lessons we can learn to better protect consumers in the future. Improving information security has to be one of our top priorities in protecting the confidentiality and integrity of our financial system. Millions of Americans are depending on us.

April 3, 2003

Opening Statement by Congressman Paul E. Gillmor
House Financial Services Committee
Subcommittee on Oversight and Investigations and Subcommittee on Financial Institutions and Consumer Credit
Hearing entitled, "Fighting Fraud: Improving Information Security"

I thank our Subcommittee Chairmen for holding this important hearing. As a result of the horrific terrorist attacks on September 11, 2001, security concerns, especially in our financial markets, have taken on new relevance.

I look forward to our evaluation of the three case studies we have before us this morning and a full review of current industry security practices. Beyond national security concerns related to fraud in the financial services industry, we need to fully discuss personal financial privacy. Throughout my years in Congress, I have been a strong defender of personal privacy, financial and otherwise.

When this issue was considered during negotiations in the 106th Congress on the Gramm-Leach-Bliley Act, the need for further safeguards to protect consumer privacy were recognized and legislative action was taken. However, clearly fraud is still taking place and our debate on this issue continues.

I thank the representatives of Teledata Communications Inc., DPI Merchant Services, and TriWest Healthcare for being with us today. Lessons can be learned from our investigation of these incidents of fraud. I look forward to any insights the law enforcement officials that have also joined us can provide.

Thank you again Chairman Bachus and Chairwoman Kelley for taking the lead on this issue. I look forward to this committee's continued discussions on personal financial privacy.

**OPENING REMARKS OF THE HONORABLE RUBÉN HINOJOSA**
**JOINT HOUSE O & I AND FINANCIAL INSTITUTIONS HEARING**
**ON**
**"FIGHTING FRAUD: IMPROVING INFORMATION SECURITY"**
**APRIL 3, 2003**

Chairman Bachus, Ranking Member Sanders, Chairwoman Kelly, and Ranking Member Gutierrez,

I want to thank you for holding this important and timely joint hearing on "Fighting Fraud: Improving Information Security." I look forward to hearing the testimony of all the witnesses, particularly their insight into the three cases we are going to discuss today:

? **Teledata Communications Inc (TCI)**, in which individuals downloaded the personal information of 30,000 individuals over a period of time and accessed reports from consumer reporting agencies using access codes assigned to several lenders;

? the **TriWest Break-In**, in which sensitive information, including medical information, was stolen off this companies computer, potentially compromising the privacy of over 500,000 military, their families and retirees; and,

? the **DPI Merchant Services** case, in which a hacker allegedly stole over 10 million Visa, MasterCard and American Express card numbers from the credit card processor.

All three of these cases are very troubling as they send a signal to the public that their personal financial and medical information is not safe. They send the signal that ID theft is fairly easy to accomplish and difficult to undo. These cases make us realize just how essential it is that we address the important issue of Identity Theft as soon as possible this Congress. I am glad that Congresswoman Hooley has formed a Task Force to accomplish this difficult task.

I want to commend the FTC for its efforts to address ID theft, especially the release of its pamphlet in both English and Spanish entitled *Identity Theft: When Bad Things Happen to Your Good Name*. I placed a hyperlink to that publication on my website for my constituents to access if they believe they are victims of Identity Theft. There is an old saying that education is the key to success. In this instance, education is the key to fraud prevention. I applaud the FTC for the workshops it provides to the public to prevent ID Theft and to protect their privacy.

I also applaud the FTC for finalizing its Gramm-Leach-Bliley Safeguards Rule, which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information. The Rule becomes effective on May 23, 2003. The Commission noted in its testimony that it expects this new Safeguards Rule to quickly become an important tool to ensure greater security for consumers' sensitive financial information. I hope this will be the case and look forward to having additional information on this rule.

It is essential that we in Congress work together with the federal agencies, the associations and

private industry to ensure that the three cases we examine today will not be repeated in the future, and to ensure that the privacy of our constituents is protected.

Thank you Mr. Chairman and Mrs. Chairwoman. I look forward to hearing the testimony of the witnesses.

**Statement of Ron Paul**

**Subcommittee on Oversight and Investigations and**

**Subcommittee on Financial Institutions and Consumer Credit**

**Hearing on "Fighting Fraud; Improving Information Security"**

04-03-02

Madam Chairwoman, thank you for holding this timely hearing on the important topic of how to prevent identity crimes. I would also like to thank the Subcommittee on Financial Institutions and Consumer Credit for participating in this hearing. However, Madam Chairwoman, I am little surprised that this hearing seems to be focusing on the private sector's efforts to protect against identity theft while ignoring how Congress' transformation of the Social Security number into a *de facto* uniform identifier facilitates identity crimes.

Since the creation of the Social Security number, Congress has authorized over 40 uses of the Social Security number as an identifier. Thanks to Congress, today no American can get a job, open a bank account, get a professional license, or even get a drivers' license without presenting their Social Security number. Federal law even requires Americans to produce a Social Security number to get a fishing license!

Because of the congressionally-mandated abuse of the Social Security number, all an unscrupulous person needs to do is obtain someone's Social Security number in order to access that person's bank accounts, credit cards, and other financial assets. Every case highlighted in the Committee's hearing memo references whether or not the thieves where successful in obtaining Social Security numbers, acknowledging the importance of the Social Security number to identity thieves.

Madam Chairwoman, the only way to ensure the federal government is not inadvertently assisting identity criminals is to stop using the Social Security number as a uniform ID. I have introduced legislation to address the American people's concerns regarding the transformation of the Social Security number into a national ID, the Identity Theft Prevention Act (HR 220). The major provision of the Identity Theft Prevention Act halts the practice of using the Social Security number as an identifier by requiring the Social Security Administration to issue all Americans new Social Security numbers within five years after the enactment of the bill. These new numbers will be the sole legal property of the recipient, and the Social Security Administration shall be forbidden to divulge the numbers for any purposes not related to the Social Security program. Social Security numbers issued before implementation of this bill shall no longer be considered valid federal identifiers. Of course, the Social Security Administration shall be able to use an individual's original Social Security number to ensure efficient transition of the Social Security system.

Madam Chairwoman, while I do not question the sincerity of those members who suggest that Congress can ensure citizens' rights are protected through legislation

restricting access to personal information, legislative "privacy protections" are inadequate to protect the liberty of Americans for several reasons. First, it is simply common sense that repealing those federal laws that promote identity theft is more effective in protecting the public than expanding the power of the federal police force. Federal punishment of identity thieves provides cold comfort to those who have suffered financial losses and the destruction of their good reputation as a result of identity theft.

Federal laws are not only ineffective in stopping private criminals; they have not even stopped unscrupulous government officials from accessing personal information. Did laws purporting to restrict the use of personal information stop the well-publicized violation of privacy by IRS officials or the FBI abuses by the Clinton and Nixon administrations?

Just this past December, thousands of active-duty soldiers and veterans had their personal information stolen, putting them at risk of identity theft. Imagine the dangers if thieves are able to obtain the universal identifier, and other personal information, of millions of Americans simply by breaking, or hacking, into one government facility or one government database?

My colleagues should remember that the federal government lacks constitutional authority to force citizens to adopt a universal identifier for health care, employment, or any other reason. Any federal action that oversteps constitutional limitations violates liberty because it ratifies the principle that the federal government, not the Constitution, is the ultimate judge of its own jurisdiction over the people. The only effective protection of the rights of citizens is for Congress to follow Thomas Jefferson's advice and "bind (the federal government) down with the chains of the Constitution."

In conclusion, Madam Chairwoman, I once again thank you and the other members of the subcommittee for holding a hearing on this important issue. However, I would hope my colleagues would turn their attention away from private efforts to prevent identity theft and address the congressionally-created root cause of the problem: the transformation of the Social Security number into a national identifier.

*Opening Statement*
*Hearing: Fighting Fraud: Improving Information Security*
*Congressman John Shadegg*

First, I would like to begin by thanking Chairman Bachus and Chairwoman Kelly for holding a hearing on improving information security. I also want to thank one of my own constituents, Mr. David McIntyre, President and CEO of TriWest Healthcare Alliance, for agreeing to testify.

My personal interest in identity theft began about five years ago when two of my constituents, Bob and JoAnn Hartle of Phoenix, Arizona, were victims of identity theft. My constituents were instrumental in getting the first state law in the nation to criminalize identity theft passed. Mr. and Mrs. Hartle suffered the devastation of identity theft when a convicted felon took Mr. Hartle's identity and made purchases totaling over $100,000. This individual also used Mr. Hartle's identity to obtain a security clearance to secure areas of Phoenix Sky Harbor International Airport and to obtain handguns using Mr. Hartle's clean record to go around the Brady gun law.

As a result of this victimization, Mr. and Mrs. Hartle were forced to spend more than four years of their lives and more than $15,000 of their own money to restore their credit because there were no federal penalties for identity theft. Their case led me to introduce a bill in the House that was eventually signed into law. The Identity Theft and Assumption Deterrence Act of 1998 gave law enforcement agencies the authority to investigate and prosecute identity theft crimes. Mr. and Mrs. Hartle also turned their unfortunate circumstance into something positive by establishing a non-profit organization to assist other victims of identity theft. Their website, www.idfraud.net is available to provide guidance to identity theft victims nationwide.

Identity theft ranges from individual instances like the Hartles' – involving small or large dollar amounts – to large organized professional crime rings. In fact, TriWest Healthcare Alliance, may well have been the victim of a professional operation. Like the Hartle's, Mr. McIntyre and his company took an unfortunate circumstance and turned it into a positive model for other companies to follow. Under Mr. McIntyre's leadership, on the morning of December 14, 2002, upon discovery of the break-in of their Phoenix office and the theft of computer hard drives containing their clients sensitive personally-identifiable information, TriWest Healthcare Alliance embarked on a journey to notify all 562,000 affected customers of the theft.

The stolen data included personally-identifiable information such as social security numbers, birth dates, and addresses from military personnel (one-quarter of whom are on active duty), retirees and family members who are served by TriWest under a contract with the Department of Defense. TriWest immediately reported the theft to the police, notified Department of Defense officials, and launched a 30-hour data run to determine what files were stolen. In addition, the company established a dedicated email address and set-up a toll-free telephone number with a three-tier response framework so customers would not experience wait times longer than one minute. TriWest mailed letters notifying victims of the theft and providing guidance on steps to take to protect their credit. TriWest also posted a $100,000 reward for information leading to the conviction of those responsible for the theft. In all, TriWest

undertook great efforts to notify the victims of the theft at a great financial expense to the company. Due to their extraordinary efforts, to date, no information from the purloined computer files have led to a single instance of identity theft.

The nature of identity theft has changed and the threat today is more likely than ever to come from breaches of data security. According to an identity-fraud manager at the Federal Trade Commission, there is a shift by identity thieves from going after single individuals to going after a mass amount of information. Law enforcement experts now estimate that half of all cases come from thefts of business databanks, as more and more information is stored in computer databases that are vulnerable to attack from hackers.

The identity theft legislation that I introduced and was signed into law in 1998 was an important first step in the road to crack-down on identity fraud crimes. However, more legislation is needed in this area to protect thieves from easily obtaining social security and credit card numbers from victims' mailboxes and waste containers left at the curb, to provide better coordination between victims and credit reporting bureaus, to establish procedures for businesses to follow in the event of a data security breach, and to provide stiffer penalties for criminals who steal and use another's identity. I look forward to hearing testimony from all of the witnesses to help identify areas in which a legislative response may be needed.

Chairman Bachus, Chairwoman Kelly, I thank you for holding a hearing on this important topic.

# PREPARED STATEMENT OF

# THE FEDERAL TRADE COMMISSION ON

# IDENTITY THEFT:

**Before the**

**HOUSE FINANCIAL SERVICES COMMITTEE**

**Washington, D.C.**

**April 3, 2003**

## I. INTRODUCTION

Mr. Chairman, and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the impact of identity theft on consumers and the importance of information security in preventing identity theft.

The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. The FTC's primary role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").[2] The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. The Commission also works extensively with private industry on ways to improve victim assistance, including providing direct advice and assistance in cases when information has been compromised. The Commission can take enforcement action when companies fail to take adequate security precautions to protect consumers' personal information.

---

[1]The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

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

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

The Identity Theft Act strengthened the criminal laws governing identity theft[3] and focused on consumers as victims.[4] Congress also recognized that coordinated efforts are essential to best serve the needs of identity theft victims because these fraud victims often need assistance both from government agencies at the national and state or local level and from private businesses. Accordingly, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.[5] Specifically, Congress directed the Commission to establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity

---

[3]18 U.S.C. § 1028(a)(7). The statute broadened "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.,* credit cards), electronic identification number or routing code, and telecommunication identifying information.

[4]Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105-274, at 4 (1998).

[5]Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g.,* FTC v. Assail, Inc., W03 CA 007 (W.D.Tx Feb. 4, 2003) (order granting preliminary injunction) (defendants alleged to have debited consumers' bank accounts without authorization for "upsells" related to bogus credit card package) and FTC v. Corporate Marketing Solutions, Inc., CIV - 02 1256 PHX RCB (D. Ariz Feb.3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. Press Release, Federal Trade Commission, FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam (January 16, 2003) (*at* http://www.ftc.gov/opa/2003/01/idpfinal.htm).

theft victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[6] To fulfill the purposes of the Act, the Commission has implemented a plan that centers on three principal components: (1) A toll-free telephone hotline, (2) the Identity Theft Data Clearinghouse (the "Clearinghouse"), a centralized database used to aid law enforcement, and (3) outreach and education to consumers, law enforcement, and private industry.

**A. Toll-free Telephone Hotline**

On November 1, 1999, the Commission established a toll-free telephone number, 1-877-ID THEFT (438-4338), for consumers to report identity theft and to receive information about identity theft. In 2002, hotline counselors added almost 219,000 consumer reports to the Clearinghouse, up from more than 117,000 in 2001. Of the 219,000 reports, almost 162,000 (74%) were complaints from actual victims of identity theft, and almost 57,000 (26%) were inquiries about identity theft generally. Despite this dramatic growth in reports, the FTC is cautious in attributing it entirely to a commensurate growth in the prevalence of identity theft. The FTC believes that the increase is, at least in part, an indication of successful outreach in informing the public of its program and the availability of assistance.

Callers to the hotline receive telephone counseling from specially trained personnel to provide them with general information about identity theft or to help them through the steps they need to take to resolve the problems resulting from the misuse of their identities. Victims are advised to: (1) Contact each of the three national consumer reporting agencies to obtain copies of

---

[6]Pub. L. No. 105-318, § 5, 112 Stat. 3010 (1998).

their credit reports and request that a fraud alert be placed on their credit reports;[7] (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated debts; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

Counselors also are trained to advise victims having particular problems about their rights under relevant consumer credit laws including the Fair Credit Reporting Act,[8] the Fair Credit Billing Act,[9] the Truth in Lending Act,[10] and the Fair Debt Collection Practices Act.[11] If the investigation and resolution of the identity theft falls under the jurisdiction of another regulatory agency that has a program in place to assist consumers, callers also are referred to those agencies.

---

[7] These fraud alerts indicate that the consumer is to be contacted before new credit is issued in that consumer's name. *See* Section II.C.(3) *infra* for a discussion of the credit reporting agencies new "joint fraud alert" initiative.

[8] 15 U.S.C. § 1681 *et seq.*

[9] *Id.* § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

[10] *Id.* § 1601 *et seq.*

[11] *Id.* § 1692 *et seq.*

**B. Identity Theft Data Clearinghouse**

The Identity Theft Act directed the FTC to log the complaints from victims of identity theft and refer those complaints to appropriate entities such as law enforcement agencies. Before launching this complaint system, the Commission took a number of steps to ensure that it would meet the needs of criminal law enforcement, including meeting with a host of law enforcement and regulatory agencies to obtain feedback on what the database should contain. Access to the Clearinghouse via the FTC's secure Web site became available in July of 2000. To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaints from other sources. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a much fuller picture of the nature, prevalence, and trends of identity theft than was previously available.[12] FTC data analysts aggregate the data to develop statistics about the nature and frequency of identity theft. For instance, the Commission publishes charts showing the prevalence of identity theft by states and by cities. Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

Since the inception of the Clearinghouse, 75 federal agencies and 549 state and local agencies have signed up for access to the database. Within those agencies, over 4500 individual

[12] Charts that summarize 2002 data from the Clearinghouse can be found at www.consumer.gov/idtheft and www.consumer.gov/sentinel.

investigators have the ability to access the system from their desktop computers twenty-four hours a day, seven days a week. The Commission actively encourages even greater participation.

One of the goals of the Clearinghouse and the FTC's identity theft program is to provide support for identity theft prosecutions nationwide.[13] To further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice and the United States Secret Service, initiated a full day identity theft training seminar for state and local law enforcement officers. Last year, the FTC held sessions in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, and Dallas. More than 600 officers have attended these seminars, representing more than 130 different agencies. This year, the FTC tentatively plans to hold similar training seminars in Phoenix, Seattle, New York, and Houston -- cities the FTC has identified as having high rates of identity theft.

The FTC staff also helps develop case leads. Now in its second year, the Commission runs an identity theft case referral program in coordination with the United States Secret Service, which assigned a special agent on a full-time basis to the Commission to assist with identity theft issues and has provided the services of its Criminal Research Specialists.[14] Together, the FTC and Secret Service staff develop preliminary investigative reports by examining significant patterns of identity theft activity in the database and refining the data through the use of additional

---

[13]The Commission testified last year in support of S. 2541, the Identity Theft Penalty Enhancement Act of 2002, which would increase penalties and streamline proof requirements for prosecution of many of the most harmful forms of identity theft. *See* Testimony of Bureau Director J. Howard Beales, Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Government Information (July 11, 2002).

[14]The referral program complements the regular use of the database by all law enforcers from their desk top computers.

investigative resources. Thereupon, the staff refer the investigative reports to appropriate Financial Crimes Task Forces located throughout the country for further investigation and potential prosecution.

**C. Outreach and Education**

The final mandate for the FTC under the Identity Theft Act was to provide information to consumers about identity theft. Recognizing that the roles of law enforcement and private industry play an important part in the ability of consumers to both minimize their risk and to recover from identity theft, the FTC expanded its mission of outreach and education to include these sectors.

(1) *Consumers*: The FTC has taken the lead in coordinating with other government agencies and organizations in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive, multi-media campaign includes print materials, media mailings, and interviews, as well as the identity theft website, located at www.consumer.gov/idtheft, which includes the publications, descriptions of common identity theft scams, and links to testimony, reports, press releases, identity theft-related state laws, and other resources.[15] The site also has a link to a web-based complaint form, allowing consumers to send complaints directly to the Clearinghouse.

The FTC's comprehensive consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*, has been a tremendous success. The 26-page booklet, now in its

---

[15]www.consumer.gov is a multi-agency "one-stop" website for consumer information. The FTC hosts the server and provides all technical maintenance for the site. It contains a wide array of consumer information and currently has links to information from more than 170 federal agencies.

fourth edition, covers a wide range of topics, including how identity theft occurs, how consumers can protect their personal information and minimize their risk, what steps to take immediately upon finding out they are a victim, and how to correct credit-related and other problems that may result from identity theft. It also describes federal and state resources that are available to consumers who have particular problems as a result of identity theft. The FTC alone has distributed more than 1.2 million copies of the booklet since its release in February 2000.[16] Last year, the FTC released a Spanish language version of the Identity Theft booklet *Robo de Identidad: Algo malo puede pasarle a su buen nombre.*

(2) *Law Enforcement*: Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described above, the staff recently joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General letting him or her know about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. The letter encourages the Attorney General to link to the consumer information and complaint form on the FTC's website and to let residents know about the hotline, stresses the importance of the Clearinghouse as a central database, and describes all of the educational materials that the Attorney General can distribute to residents. North Carolina took the lead in availing itself of the Commission's resources in putting together for its resident victims a package of assistance that includes the ID Theft Affidavit (*see* Section II.C.(3)), links to the FTC website, and its own booklet containing

[16]Other government agencies, including the Social Security Administration, the SEC, and the FDIC also have printed and distributed copies of *Identity Theft: When Bad Things Happen to Your Good Name.*

information from *Identity Theft: When Bad Things Happen to Your Good Name.* Through this initiative, the FTC hopes to make the most efficient use of federal resources by allowing states to take advantage of the work the FTC has already accomplished and at the same time continuing to expand the centralized database of victim complaints and increase its use by law enforcement nationwide. Other outreach initiatives include: (1) Participation in a "Roll Call" video produced by the Secret Service, which will be sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims; and (2) the redesign of the FTC's website to include a section for law enforcement with tips on how to help victims as well as resources for investigations. The FTC will launch the new web site shortly.

(3) *Private Industry*:

(a) Victim Assistance: Because identity theft victims spend significant time and effort restoring their good name and financial records, the FTC devotes significant resources to conducting outreach with the private sector on ways in which victim assistance procedures can be improved. One such initiative arose from the burdensome requirement for victims to complete a different fraud affidavit for each different creditor when the identity thief opened or used an account in the victim's name.[17] To reduce that burden, the FTC worked with private industry and consumer advocates to create a standard form for victims to use in absolving identity theft debts with each of the creditors with whom identity thieves had opened accounts. From its release in August 2001 through February 2003, the FTC has distributed more than 264,000 print copies of

[17]*See ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

the ID Theft Affidavit. There have also been more than 351,000 hits to the Web version. The affidavit is available in both English and Spanish.

Another initiative is the development of a "joint fraud alert" among the three major credit reporting agencies ("CRAs"). This initiative will allow the CRAs to share among themselves requests from identity theft victims that fraud alerts be placed on their consumer reports and copies of their reports be sent to them, thereby eliminating the victim's need to contact each of the three major CRAs separately. A pilot program is expected to begin this month.

(b) Information Security Breaches: Additionally, the FTC is working with institutions that maintain personal information to identify ways to help keep that information safe from identity theft. Last April, the FTC invited representatives from financial institutions, credit issuers, universities and retailers to a one day informal roundtable discussion of ways to prevent access to personal information in employee and customer records. The FTC will soon publish a self-audit guide to make businesses and organizations of all sizes more aware of how they are managing personal information and to aid them in assessing their security protocols.

As awareness of the FTC's role in identity theft has grown, businesses and organizations who have suffered compromises of personal information have begun to contact the FTC for assistance. For example, in the cases of TriWest[18] and Ford/Experian,[19] in which massive numbers of individuals' personal information was taken, the Commission provided advice on notifying those individuals and what steps they should take to protect themselves. From these experiences,

---

[18]Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. TIMES, Jan. 12, 2003, § 1 (Late Edition), at 12.

[19]Kathy M. Kristof and John J. Goldman, *3 Charged in Identity Theft Case*, LA TIMES, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1.

the FTC developed a business record theft response kit that will be posted shortly on the identity theft web site. The kit includes the steps to take in responding to an information compromise and a form letter for notifying the individuals whose information was taken. The kit provides advice on the type of law enforcement agency to contact, depending on the type of compromise, business contact information for the three major credit reporting agencies, suggestions for setting up an internal communication protocol, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know. Organizations are encouraged to print and include copies of *Identity Theft: When Bad Things Happen to Your Good Name* with the letter to individuals.

The FTC particularly stresses the importance of notifying as soon as possible individuals whose information has been taken so that they can begin to take steps to limit the potential damage to themselves. Individuals who place a fraud alert promptly have a good chance of preventing, or at least reducing, the likelihood that the theft of their information will turn into the actual misuse of their information. Prompt notification also alerts them to review their credit reports and to keep watch for the signs of identity theft. In the event that they should become victims, they can quickly take action to clear their records before any long-term damage is done. In addition to providing the business record theft response kit, FTC staff can provide individual assistance and advice, including review of consumer information materials for the organization and coordination of searches of the Clearinghouse for complaints with the law enforcement officer working the case.

## III. THE FEDERAL TRADE COMMISSION'S ROLE IN INFORMATION SECURITY

In addition to providing assistance to victims of identity theft, the Commission also examines security precautions involving consumers' personal information to determine whether law enforcement may be appropriate. If so, the Commission has two valuable legal tools to work with: Section 5 of the FTC Act,[20] which prohibits unfair and deceptive acts or practices, and, starting in May of this year, the Commission's Gramm-Leach-Bliley Safeguards Rule (the "Safeguards Rule" or the "Rule").[21]

**A. Law Enforcement Under Section 5**

One of the mainstays of the Commission's privacy program is the enforcement of promises that companies make to consumers about privacy, and in particular, the precautions they take to ensure the security of consumers' personal information. The Commission currently enforces such promises both online and offline. The Commission is particularly concerned about breaches involving sensitive information because they put consumers at the greatest risk of identity theft and other harms.

Last August, the Commission announced a settlement with Microsoft regarding misleading claims made by the company about the information collected from consumers through its Passport services – Passport, Passport Wallet, and KidsPassport.[22] Passport is a service that collects information from consumers and then allows them to sign in at any participating site using a single name and password. Passport Wallet collects and stores consumers' credit card numbers, and

---

[20] 15 U.S.C. § 45.

[21] 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[22] The Commission's final decision and order in the Microsoft case is available at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf. The Commission's complaint is available at http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf.

billing and shipping addresses, so that consumers do not have to input this information every time they make a purchase from a site. Kids Passport was promoted as a way for parents to create accounts for their children that limited the information that could be collected from them.

The Commission's complaint alleged that Microsoft misrepresented the privacy afforded by these services, including the extent to which Microsoft kept the information secure. For example, in various online statements, Microsoft said that the Passport service "achieves a high level of Web Security by using technologies and systems designed to prevent unauthorized access to your personal information." In fact, the Commission alleged that Microsoft failed to employ reasonable and appropriate measures to protect the personal information collected in connection with these services because it failed to: (1) implement procedures needed to prevent or detect unauthorized access; (2) monitor the system for potential vulnerabilities; and (3) perform appropriate security audits or investigations.

The Commission's order against Microsoft contains strong relief that will provide significant protections for consumer information. First, it prohibits any misrepresentations about the use of and protection for personal information. Second, it requires Microsoft to implement a comprehensive information security program similar to the program required under the FTC's Gramm-Leach-Bliley Safeguards Rule, which is discussed below. Finally, to provide additional assurances that the information security program complies with the consent order, Microsoft must have its program certified as meeting or exceeding the standards in the order by an independent professional every two years. The provisions of the order will expire after 20 years.

Microsoft is an important case because the settlement required that the company adhere to its security promises even in the absence of a known breach of the system. The Commission

found even the potential for injury actionable when sensitive information and security promises were involved, and when the potential for injury was significant. This determination is an extremely important principle. It is not enough to make promises about protecting personal information, and then just hope that nothing bad happens or, if it does, that nobody finds out. Fulfilling privacy and security promises requires affirmative steps to ensure that personal information is appropriately protected from identity theft and other risks to consumers' personal information.

The Microsoft case followed on a similar case the Commission settled earlier last year against Eli Lilly.[23] The Lilly case also involved alleged misrepresentations regarding the security provided for sensitive consumer information – in that case, consumers' health information. Like Microsoft, Lilly made claims that it had security measures in place to protect the information collected from consumers on its website. As in Microsoft, the Commission charged Lilly with failing to have reasonable measures in place to protect the information.

Specifically, in sending an e-mail to Prozac users who subscribed to a service on the site, Lilly put all of the consumers' email addresses in the "To" line of the e-mail, essentially disclosing to all users the identities of all of the other Prozac users. The Commission's complaint alleged that this happened because Lilly failed, among other things, to provide appropriate training and oversight for the employee who sent the email and to implement appropriate checks on the process of using sensitive customer data. The order in the Lilly case prohibits the misrepresentations and, as in Microsoft, requires Lilly to implement a comprehensive information security program.

---

[23] The Commission's final decision and order against Eli Lilly is available at http://www.ftc.gov/os/2002/05/elililly do.htm. The complaint is available at http://www.ftc.gov/os/2002/05/elililly cmp.htm.

It is important to note that the Commission is not simply saying "gotcha" for security breaches. While a breach may indicate a problem with a company's security, breaches can happen even when a company takes all reasonable precautions. In such instances, the breach does not necessarily violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances. That is the approach the Commission took in these cases and in its Gramm-Leach-Bliley Safeguards Rule, and the approach it will continue to take.

**B. GLB Safeguards Rule**

Last May, the Commission finalized its Gramm-Leach-Bliley Safeguards Rule, which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information. On May 23, 2003, the Rule becomes effective and the Commission expects that it will quickly become an important tool to ensure greater security for consumers' sensitive financial information. Whereas Section 5 authority derives from misstatements particular companies make about security, the Rule requires a wide variety of financial institutions to implement comprehensive protections for customer information – many of them for the first time. The Rule could go far towards reducing risks to this information, including identity theft.

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. Due to the wide variety of different entities covered, the Rule requires a plan that takes into account each entity's particular circumstances – its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

As part of its plan, each financial institution must: (1) designate one or more employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) design and implement a safeguards program, and regularly monitor and test it; (4) hire appropriate service providers and contract with them to implement safeguards; and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards. The Safeguards Rule requires businesses to consider all areas of their operation, but identifies three areas that are particularly important to information security: employee management and training; information systems; and managing system failures.

The Commission has already issued guidance to businesses covered by the Safeguards Rule to help them understand the Rule's requirements.[24] Commission staff are currently meeting with trade associations and companies to find out how industry is progressing in coming into compliance with the Rule, to discuss areas in which additional FTC guidance might be appropriate, and to gain a better understanding of how the Rule will affect particular industry segments. When the Rule becomes effective, the Commission plans to conduct sweeps to assess compliance within various covered industry segments.

**C. Education and Workshops**

The FTC also plays a role in improving security and reducing the risks to personal information by fostering dialogue and educating the public on security issues. For example, the

---

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

Commission held a workshop last May to examine the security of consumer information – both as maintained by consumers on their own computers and by businesses in their systems.[25]

The main messages from the workshop are: (1) That consumers need greater education about steps they can take to protect their information; (2) that manufacturers, ISPs, and other businesses need to make it easier for consumers to protect themselves; and (3) that the government and private sector should work together to create a "culture of security" for consumers and businesses. Since then, the Commission has launched a major initiative to educate consumers and businesses about security. The Commission created a new mascot for this effort, Dewie the Turtle, who has his own web site at www.ft.gov/infosecurity that offers practical tips for staying secure online; complying with the Commission's Safeguards Rule; staying secure when using dial up or broadband access; and other resources available to consumers.

Finally, in May and June of this year, the Commission will host two workshops focusing on the role technology plays for both consumers and businesses in protecting personal information.[26] A number of products promise to help consumers control their sensitive information and guard against internal and external threats. Similarly, there are an increasing number of products designed to help businesses manage the consumer information they maintain and ensure that it is secure. Despite the widespread availability of these products, however, it is unclear just how much consumers and businesses are using them and whether they are meeting consumer and business needs in this area. The Commission's workshops will foster a wide-

---

[25] Additional information about the workshop is available at http://www.ftc.gov/bcp/workshops/security/index.html.

[26] Additional information about the workshop is available at http://www.ftc.gov/bcp/workshops/technology/index.html.

ranging discussion on these issues, with the goal of gaining a better understanding of whether technology is being used effectively to protect personal information.

## IV. CONCLUSION

Large scale security breaches place substantial costs on individuals and businesses. The Commission, through its education and enforcement capabilities, is committed to reducing these breaches as much as possible. The Commission will continue its efforts to assist criminal law enforcement with their investigations. Prosecuting perpetrators sends the message that identity theft is not cost-free. Finally, the Commission knows that as with any crime, identity theft can never be completely eradicated. Thus, the Commission's program to assist victims and work with the private sector on ways to facilitate the process for regaining victims' good names will always remain a priority.

# FIGHTING FRAUD: IMPROVING INFORMATION SECURITY

## TESTIMONY OF JOHN J. BRADY
## VICE PRESIDENT, MERCHANT FRAUD CONTROL
## MASTERCARD INTERNATIONAL

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

April 3, 2003

Good morning Chairman Bachus, Chairwoman Kelly, Mr. Sanders, Mr. Gutierrez, and members of the subcommittees. My name is John Brady and I am the Vice President for Merchant Fraud Control at MasterCard International in Purchase, New York. MasterCard is a global organization comprised of more than 15,000 financial institutions that are licensed to use the MasterCard service marks in connection with a variety of payments systems. For example, these member financial institutions issue payment cards to consumers and contract with merchants to accept such cards. MasterCard provides the networks through which the member financial institutions interact to complete payment transactions—MasterCard itself does not issue payment cards, nor does it contract with merchants to accept those cards. It is my pleasure to appear before you this morning to discuss the important topic of fighting fraud and safeguarding financial information.

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 MasterCard, and we have a team of experts devoted to maintaining the integrity and security of our payment systems. We are 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 Federal Bureau of Investigation, the Federal Trade Commission, the U.S. Postal Inspection Service, and others. MasterCard also fields calls from local law enforcement every day. MasterCard believes its success in fighting fraud is perhaps best demonstrated by noting that our fraud rates are at historically low levels.

### 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. MasterCard's information security program is comprehensive, and we continually update it to ensure that our program remains strong. Our member 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 member 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 member 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 member 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 member, and any third party acting on behalf of such member, to safeguard transaction and account information. Not only must our member 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.

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, 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 accounts. 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 on-line and elsewhere 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*

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 credit 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 credit card. MasterCard cards have the full 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 act similar to a PIN number for the credit card and can be used to ensure that the person presenting the credit card number actually has possession of the credit 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 both the name and 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 "name as it appears on the card" and billing address. At the time of payment, the merchant submits the consumer's name and billing address into the MasterCard system to verify with the card issuer that the name and 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 relatively new service that allows issuers to provide added security to their cardholders when the 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. When the cardholder correctly enters 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 not go through.

*"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, in part, through the use of data provided by issuers of MasterCard regarding fraud-related transaction information. For example, data regarding fraudulent merchants, transactions, and other patterns of activity is incorporated in the SAFE program for use by MasterCard and its members. 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 member financial institutions use this data to take the appropriate precautions or otherwise react to the trends as necessary. The SAFE program also allows us to identify potentially fraudulent actors relatively early in the process, before the problem escalates.

*Site Data Protection Service*

MasterCard Site Data Protection Service (SDP) is a multi-tiered, comprehensive set of global e-commerce/financial security services designed to help protect the web sites of its members and their on-line merchants from hack and attack. MasterCard designed SDP to be a cost-effective diagnostic tool for members and merchants to allow them to understand any systems vulnerabilities they may have. Furthermore, SDP also recommends actions that can be taken to reduce the potential systems vulnerabilities.

*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, or perhaps canceling the account and reissuing a new card and account number to the consumer. MasterCard also assists the issuer in monitoring the account usage in order to detect patterns of fraud.

*Issuers Clearinghouse Service*

MasterCard requires its member financial institutions in the U.S. to participate in the Issuers Clearinghouse Service (ICS), a system built using data provided by issuers regarding, among other things, the fraudulent use of consumer data. More specifically, MasterCard's U.S. members provide ICS with data regarding customer addresses, phone numbers, and social security numbers that have been associated with fraudulent activity. Furthermore, MasterCard members are required to access ICS in connection with each application to open a MasterCard

account. The ICS database allows MasterCard and its members to detect suspicious activity and to prevent consumer harms, such as identity theft. For example, the centralized ICS database would allow MasterCard and its members 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 members would be provided this data if they received an application with the same social security number or address and the member could evaluate it and take appropriate action.

A Recent Example of MasterCard's Efforts

I have described some of MasterCard's efforts to fight fraud and secure our systems. I would now like to discuss a recent example of how we address problems when they occur. There was a recent incident involving a data processor called Data Processing International (DPI). DPI was acting as a service provider to a MasterCard member bank in Ohio, which in turn was providing bankcard processing services to merchants. These services include processing the merchants' payment card transactions for submission into the appropriate payment systems. Earlier this year, DPI detected that someone had obtained unauthorized access to DPI's system. Although it is not clear at this point how much data the hacker successfully exported from the DPI system, we do know the hacker potentially had access to approximately 10 or 11 million Visa, Discover, American Express, and MasterCard payment card account numbers and expiration dates. Approximately 4 million of these account numbers were MasterCard account numbers.

Once DPI realized that someone had hacked their system, DPI took action. In addition, DPI and the bank quickly notified the U.S. Secret Service and the FBI as well as MasterCard and other affected payment card companies. MasterCard immediately took decisive action to protect its systems, its members, and, most importantly, MasterCard cardholders from fraudulent activity related to this breach. MasterCard interviewed the appropriate people at DPI, including the CEO, in order to determine the nature and scope of the breach. MasterCard gathered the card numbers involved and forwarded them via the MasterCard Alert system to the appropriate issuers. MasterCard also took steps to ensure that DPI had hired the appropriate third parties to investigate the situation, and MasterCard hired a third-party forensic firm to act on MasterCard's behalf during the investigation. MasterCard is continuing to review DPI's and the bank's information security program to ensure that they meet our standards.

MasterCard has been in ongoing contact with the issuers of the card numbers that may have been accessed. I am pleased to say that based on data we have analyzed, it does not appear that these numbers have been involved with unusual activity as a result of the breach at DPI. We believe that our success in mitigating any consumer harms as a result of the DPI hack is based on many factors. First, MasterCard has worked closely with law enforcement. Law enforcement has done a commendable job in investigating this breach and the investigation continues. Second, MasterCard's numerous anti-fraud initiatives, such as AVS and the added card security features, make it difficult for the hacker to make use of any account numbers he or she may have obtained without additional information.

Although it appears that the incident involving DPI has not resulted in any fraudulent activity, that is not to say that MasterCard has not encountered situations where an account is

used in fraudulent ways. In these instances, MasterCard works closely with the affected issuer to monitor the card usage data. MasterCard uses this data and works with the issuer and the appropriate law enforcement agency in order to apprehend the criminal. Of course, the issuer of the MasterCard card also closes the account and, under our Zero Liability policy, the cardholder is not held liable for any of the fraudulent activity on the account. The issuer also provides the cardholder with a new MasterCard card and account number.

Conclusion

MasterCard continually strives to provide its members and MasterCard 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, members, 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 Mr. Timothy Caddigan**

**Special Agent in Charge - Financial Crimes Division**
**U.S. Secret Service**

**Before**

**The House Financial Services Committee**
**Subcommittee on Financial Institutions and Consumer Credit**
**and the Subcommittee on Oversight and Investigations**

**U.S. House of Representatives**

**April 3, 2003**

Chairman Bachus, Chairwoman Kelly, Congressman Sanders, Congressman Gutierrez and members of both subcommittees, thank you for inviting me to be part of this distinguished panel, and the opportunity to address the committee regarding the Secret Service's efforts to combat cyber crime and protect our nation's financial and critical infrastructures.

Let me also take this opportunity to thank Chairman Oxley, Congressman Frank and all members of the full committee for their longstanding support of the Secret Service and the interest this committee has conveyed in our mission, our programs and our employees.

As you know, the Secret Service was created just after the conclusion of the Civil War to address the burgeoning problem of counterfeit currency. At that time, it was estimated that approximately one-third of all currency in circulation was counterfeit, and the government recognized the urgent need to address this issue in order to maintain the public's confidence in our currency. In effect, the Secret Service was engaged in an effort to protect a vital governmental function long before any notion of critical infrastructure protection had emerged.

Today, the Secret Service continues to suppress counterfeit currency as part of its traditional role but also now includes fighting cyber crime as part of our core mission to safeguard the integrity of this nation's financial payment systems. Over time, modes and methods of payment have evolved and so has our investigative mission. Computers and other "chip" devices are now the facilitators of criminal activity or the target of such. The perpetrators involved in the exploitation of such technology range from traditional fraud artists to violent criminals -- all of whom recognize new opportunities and employ anonymous methods to expand and diversify their criminal portfolio.

In this era of change, one constant that remains is our close working relationship with the banking and financial sectors. We developed this history of cooperation with the industry as a result of our unique responsibilities as a law enforcement bureau of the Department of the Treasury for the last 137 years. Even as a part of the new Department of Homeland Security, those relationships continue to grow and prosper as we continue to work with the Department of the Treasury and the financial sector to protect the banking and financial infrastructure.

Mr. Chairman, there is no shortage of information, testimony, or anecdotal evidence regarding the nature and variety of cyber-based threats to our banking and financial sectors and the need to create effective solutions. There is, however, a scarcity of information regarding successful models to combat such crime in today's high tech environment. This is where the Secret Service can make a significant contribution to the discussion of successful law enforcement efforts to combat cyber crime -- efforts that are central to the mission of critical infrastructure protection.

The concept of task forces has been around for many years and these groups have been employed at many levels within the law enforcement community. However, traditional task forces have consisted primarily of law enforcement personnel to the exclusion of other parties who could make significant contributions. The New York Electronic Crimes Task Force developed a new approach which enabled local, state, and federal law enforcement officials to collaborate with prosecutors, private industry and academia to fully maximize what each has to offer in furtherance of a common goal -- the protection of America's financial infrastructure.

The Secret Service applied this new approach to our own investigate mission and developed a highly effective formula for combating high tech crime, a formula that has been successfully implemented by the New York Electronic Crimes Task Force (NYECTF). While the Secret Service leads this innovative effort, we do not control or dominate the participants or the investigative agenda of the task force. Rather, the task force provides a productive framework and collaborative crime-fighting environment in which the resources of its participants can be combined to effectively and efficiently make a significant impact on electronic crimes. Other law enforcement agencies bring additional criminal enforcement jurisdiction and resources to the task force while representatives from private industry, such as telecommunications providers, for instance, bring a wealth of technical expertise.

Arrests have traditionally been the ultimate goal of law enforcement investigations, but we believe there <u>must</u> be additional means that are just as effective, if not more effective, in the battle against cyber criminals. As such, the new Electronic Crimes Task Force (ECTF) model stresses prevention through partnership. We focus on the mitigation of damage and the quick repair of any damage or disruption to get the system operational as soon as possible after an intrusion occurs. This approach requires the detailed planning and preparation that comes from the relationships, partnerships and level of trust that

have been developed through the ECTFs between law enforcement, academia and the private sector.

The NYECTF, established in 1995, has brought together 50 different federal, state and local law enforcement agencies as well as prosecutors, academic leaders and over 100 different private sector corporations. The wealth of expertise and resources that reside in this task force coupled with unprecedented information sharing yields a highly mobile and responsive machine. In task force investigations, local law enforcement officers hold supervisory positions and representatives from other agencies regularly assume the role of lead investigator. These investigations encompass a wide range of computer-based criminal activity, involving e-commerce frauds, intellectual property violations, identity crimes, telecommunications fraud, and a wide variety of computer intrusion crimes that affect a variety of infrastructures.

Pursuant to Public Law 107-56, the USA/PATRIOT Act of 2001, the Secret Service was authorized to establish a nationwide network of ECTFs, based on our New York model. Subsequently, we have organized task forces in Boston, Charlotte, Chicago, Los Angeles, Miami, San Francisco, Washington D.C., and Las Vegas. These locations were selected based on the presence and support of financial, information technology and government entities; the perceived need for such a task force in that area; the incidence of hi-tech criminal activity; and our interest in a balanced geographic distribution across the country.

An important component in our investigative response to cyber crime is the Electronic Crimes Special Agent Program (ECSAP). This program is comprised of approximately 175 special agents who have received extensive training in the forensic identification, preservation, and retrieval of electronically stored evidence. Special Agents entering the program receive advanced training in all areas of electronic crimes, with particular emphasis on computer intrusions and forensics. ECSAP agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence, including computers, personal data assistants, telecommunications devices, electronic organizers, scanners and other electronic paraphernalia.

Since 2000, our ECSAP agents have completed over 3,463 examinations on computer and telecommunications equipment. Although the Secret Service did not track the number of exams performed for other law enforcement agencies during this period, it is estimated that some 10 to 15 percent of these examinations fell in this category. Many of the examinations were conducted in support of other agencies' investigations, such as those involving child pornography or homicide cases, simply because the requesting agency did not have the resources to complete the examination itself.

We provide physical assistance on a regular basis to other departments, often dispatching ECSAP agents overnight to the requesting venue to perform computer-related analyses or technical consultation. In fact, so critical was the need for even basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to

Searching and Seizing Electronic Evidence" which is designed for the first responder, line officer and detective alike.

We have also worked with these same partners in producing the interactive, computer-based training program known as "*Forward Edge*," which takes the next step in training officers to conduct electronic crime investigations. *Forward Edge* is a CD-ROM that incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the training program and are immediately accessible for instant implementation.

Thus far, we have dispensed over 300,000 "Best Practices Guides" to local and federal law enforcement officers and have distributed, free of charge, over 20,000 *Forward Edge* training CDs.

Let me relate the Secret Service's mission in fighting cyber crime to the bigger picture of critical infrastructure protection and partnerships. We target electronic crime as it may affect the integrity of our nation's financial payment and banking systems, one of our most important critical infrastructures. Yet our efforts to combat cyber attacks, which target the information and communications systems that support the financial sector, are part of a more comprehensive critical infrastructure protection scheme. The whole notion of infrastructure protection embodies an assurance and confidence in the delivery of critical functions and services that in today's world are increasingly interdependent and interconnected. Moreover, the public's confidence is lost if such delivery systems and services are unreliable or unpredictable, regardless of the cause of the problem.

The Secret Service has focused its efforts with regard to information security within a relatively narrow spectrum defined by its jurisdictional authorities and our financial payment systems. In this respect the Secret Service ECTF initiative has played, and will continue to play, an increasingly critical role.

The Critical Systems Protection Initiative (CSPI), a collaborative effort between the Secret Service and Carnegie-Mellon University, is working to establish standards, guidelines and methodologies to incorporate a "cyber security" component to our vital mission of protecting our highest elected leaders and events of national significance. This initiative is truly groundbreaking in that it considers both the physical vulnerabilities of a venue for security requirements as well as a "fourth dimension" -- the supporting information technology infrastructure. We recognize that a well-executed cyber attack against a weak technology or support infrastructure system can render an otherwise sound physical security plan vulnerable and inadequate.

A prime example of this was the implementation of both physical and cyber security plans at the 2002 Winter Olympics in Salt Lake City, Utah. The 2002 Winter Games represented the largest coordinated effort in American law enforcement history, and as part of this effort a number of our agents and specialists were specifically assigned to the

task of preventing, investigating and managing numerous intrusion attempts and email threats. These same principles and practices, updated as they adjust to advances in technology, will be implemented during future national events, such as the 2004 Democratic and Republican National Conventions.

It should also be noted that all deliberate infrastructure attacks are also cyber crimes and are likely to be first addressed by law enforcement personnel, both federal and local, in the course of routine business. In fact, there does not appear to be any sort of universal agreement as to when a "hack" or network intrusion rises to the threshold of an infrastructure attack, but we would all probably recognize one when it reached catastrophic proportions.

Given this interplay between computer-based crimes and national security issues, the investigation of electronic attacks against the financial sector is a significant component of larger plans for the protection of our nation's critical infrastructures. When we arrest a criminal who has breached and disrupted a sensitive communications network and are able to restore the normal operation of the host -- be it a bank, telecommunications carrier, or medical service provider -- we believe we have made a significant contribution towards assuring the reliability of the critical systems that the public relies upon on a daily basis.

The Secret Service believes there is value in sharing information during the course of our investigations with both those in the private sector and academia who are devoting substantial resources to protecting their networks and researching new solutions. When sharing such information, the Secret Service takes appropriate steps to protect privacy concerns and ensure that there are no conflicts with prosecutorial issues. I would add that there are many opportunities for the law enforcement community to share information with our private sector counterparts without fear of compromise. The Secret Service recognizes the need for a "paradigm shift" with respect to this type of information sharing between law enforcement and our private sector and academic counterparts.

Law enforcement in general is not sufficiently equipped to train the masses nor can it compete with academic institutions of higher learning in the area of research and development. However, our partnerships with industry and academia have demonstrated that this can be an integral part of the solution. Partnerships are a very popular term in both government and the private industry these days and everyone agrees that there is great utility in such an approach. Unfortunately, however, partnerships cannot be legislated, regulated, or stipulated. Nor can partnerships be purchased, traded or incorporated. Partnerships are voluntarily built between people and organizations that recognize the value in joint collaboration toward a common end. They are fragile entities, which need to be established and maintained by all participants and built upon a foundation of trust.

The Secret Service, by virtue of the protective mission for which we are so well known, has always emphasized discretion and trust in executing our protective duties. Our protective model stresses prevention, and this is achieved through partnerships that we

develop with law enforcement and private industry. We learned long ago that our agency needed the full support and confidence of local law enforcement and certain key elements of the private sector to create and maintain a successful and comprehensive security plan. Furthermore, we are also keenly aware that we need to maintain a trusted relationship with our protectees so that we can work with them and their staffs to maintain the delicate balance between security and personal privacy.

This long history of discretion and trust naturally permeates our investigative mission where we enjoy quiet successes with our private sector partners. We have successfully investigated many significant cases with the help of our private sector partners, such as network intrusions and compromises of critical information or operating systems. In such cases, even though we have significant technical expertise, we still rely on our private sector counterparts to collaborate with us in identifying and preserving critical evidence to solve the case and bring the perpetrator to justice. Equally important in such cases is conducting the investigation in a manner that avoids unnecessary disruption or adverse consequences to the victim or business. With the variety of operating platforms and proprietary operating systems in the private sector, we could not accomplish these objectives without the direct support of our private sector counterparts. Our ECTFs across the country have been working hard at maintaining and building this trust that has developed between law enforcement, private industry and academia.

Let me share with you some insights regarding an ongoing case that our Omaha Resident Office is investigating in conjunction with our Chicago, New York and San Francisco Electronic Crimes Task Forces. The case, which came to our attention in early February through our contacts in the credit card industry, involves an unlawful intrusion into the computer system of a third-party credit card processor. This company is responsible for processing the credit card transactions of companies such as Visa, MasterCard, American Express and Discover. We believe that multiple machines combined to attack this processor's computer system and unlawfully seize well over 10 million credit card numbers, along with expiration dates, from the company's electronic files.

Our investigation, with the involvement of the Federal Bureau of Investigation, determined that these multiple servers were located both within and outside the United States. The Secret Service is completing electronic forensic examinations and is working with foreign authorities in gathering further evidence concerning this attack.

Mr. Chairman, that concludes my prepared statement, and I would be happy to answer any questions that you or other members of the subcommittees may have.

Testimony by
James E. Farnan, Deputy Assistant Director, Cyber Division,
Federal Bureau of Investigation,
before the
House Financial Services Committee, Subcommittees on
Financial Institutions and Consumer Credit, and
Oversight and Investigations
on April 3, 2003

Thank you for inviting me here today to testify on the topic, "Fighting Fraud: Improving Information Security." Holding this hearing demonstrates your commitment to improving the security of our Nation's information systems and this committee's leadership on this issue in Congress. Our work here is vitally important because the stakes involved are enormous. My testimony today will address the activities of the FBI's Cyber Division as they relate to a broad spectrum of criminal acts involving fraud and information security.

Today there are over 180 million computer users in the United States alone. There are more than 600 million worldwide, and the number is growing. Many of these users are connecting to the Internet, communicating, conducting business, managing financial affairs, searching for information and, unfortunately, committing crimes.

**Cyber Vulnerabilities**

Anyone with a basic computer interest is probably aware of the existence of security vulnerabilities, at least in a general sense, in our networks and computers. These vulnerabilities are widely discussed in the media. Using a simple Internet search, a 12 year old could locate a variety of hacker tools, then download and implement them. When we first saw the dramatic increase in home computers in early 1990s, we did not worry about attacks on our family computers. Most casual users were not aware that security vulnerabilities even existed. Today, we worry about our systems getting hit with viruses, worms and Trojans. Companies secure web sites and web pages against attacks and defacements. Consumers are concerned that companies are not maintaining adequate security on our personal and financial information as we hear weekly news reports about hackers and new intrusions.

American consumers and businesses increasingly are relying on the Internet to complete transactions. E-commerce is growing in all sectors of the U.S. economy. Most e-commerce transactions are business-to-business (B2B), but e-commerce retail sales reached $46 billion in 2002,

up from $36 billion in 2001.[1] When Internet users—be they businesses or consumers—are crippled by Internet fraud schemes, the viability of e-commerce is compromised.

Computer intrusions are a different category from most fraud schemes. Many intrusions are never reported because companies fear a loss of business from reduced consumer confidence in their security measures or from a fear of lawsuits. Most of the outsider-intrusions cases opened today are the result of a failure to patch a known vulnerability for which a patch has been issued. Theft of consumer information from a computer system can only be facilitated two ways: by insiders or by outside hackers. Insiders have various motivations, including retribution and money. Outsiders are usually motivated by challenge and/or greed.

The National Research Council issued a report in 2001 titled, "Cybersecurity Today and Tomorrow: Pay Now or Pay Later,"[2] If you have not seen the report, I would urge you to obtain a copy. The report makes a number of significant points and general observations, including a key one for this Hearing:

> "Note also that an attacker...may be able to exploit a flaw accidentally introduced into a system. System design and/or implementation that is poor by accident can result in serious security problems that can be deliberately target in a penetration attempt by an attacker."[3]

If security on a system is inadequate, and someone chooses to exploit the weaknesses, consequences are inevitable. According to the report, there are three things that can go wrong with a computer system or network[4]:

1. It can become unavailable or very slow. That is, using the system or network at all becomes impossible, or nearly so.

2. It can become corrupted, so that it does the wrong thing or gives wrong answers. For example, data stored on the computer may become different from what it should be, as would be the case if medical or financial records were improperly modified.

---

[1]Jennifer Gerlach, ARS Analyst Outlook, January 2003, La Jolla, ARS, Inc.

[2]Computer Science and Telecommunications Board (CSTB), National Research Council, Cybersecurity Today and Tomorrow: Pay Now or Pay Later, (Washington, DC, National Academy Press, 2001)

[3]CSTB, page 4

[4]CSTB, page 3

3. It can become leaky. That is, someone who should not have access to some or all of the information available through the network obtains such access.

When one of these things happen, the FBI is in a unique position to respond because it is the only Federal agency that has the statutory authority, expertise, and ability to combine the counterterrorism, counterintelligence, and criminal resources needed to effectively neutralize, mitigate, and disrupt illegal computer-supported operations.

**The FBI's Cyber Division**

The FBI's reorganization of the last two years included the goal of making our cyber investigative resources more effective. In 2002, the reorganization resulted in the creation of the FBI's Cyber Division.

The Cyber Division addresses cyber threats in a coordinated manner, allowing the FBI to stay technologically one step ahead of the cyber adversaries threatening the United States. The Cyber Division addresses all violations with a cyber nexus, which often have international facets and national economic implications. The Cyber Division also simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence, and other criminal investigations when aggressive technological investigative assistance is required. The Cyber Division will ensure that agents with specialized technology skills are focused on cyber related matters.

At the Cyber Division we are taking a two-tracked approach to the problem. One avenue is identified as traditional criminal activity that has migrated to the Internet, such as Internet fraud, on-line identity theft, Internet child pornography, theft of trade secrets, and other similar crimes. The other, non-traditional approach consists of Internet-facilitated activity that did not exist prior to the establishment of computers, networks, and the World Wide Web. This encompasses "cyber terrorism," terrorist threats, foreign intelligence operations, and criminal activity precipitated by illegal computer intrusions into U.S. computer networks, including the disruption of computer supported operations and the theft of sensitive data via the Internet. The FBI assesses the cyber-threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes is on the rise.

To accomplish its mission, the Cyber Division will form and maintain public/private alliances in conjunction with enhanced education and training to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities. The FBI will also maximize the success of cyber investigations through awareness and exploitation of emerging technology.

To support this mission we are dramatically increasing our cyber training program and international investigative efforts. Consequently, specialized units are now being created at FBI Headquarters to provide training not only to FBI cyber squads, but also to the other agencies

participating in existing or new cyber-related task forces in which the FBI is a participant. This training will largely be provided to investigators in the field. A number of courses will be provided at the FBI Academy at Quantico.

A typical case will come to the FBI through the Internet Fraud Complaint Center (IFCC), In its fourth year of operation, IFCC has proven to be a very successful clearinghouse, receiving over 75,000 complaints in 2002 on crimes ranging from identity theft and computer intrusions to child pornography.

If the IFCC received an intrusion report from a company in Birmingham, Alabama, we would first attempt to locate where the intrusion took place. That same company may have its servers in Minneapolis, while the intruder is routing attacks through Internet providers in California and Europe. If the servers in Minneapolis were hacked, the Minneapolis Cyber Crime Task Force would be assigned the lead on the case. The leads could start in California, but end up in Eastern Europe, Nigeria or even back to Birmingham, if an insider was involved. One of the FBI's Computer Analysis Response Teams (CART) would be called upon to preserve computer forensic evidence, and that evidence could be forwarded to one of our new Regional Crime Forensic Labs, now located in Chicago, Dallas and San Diego. The Lab would determine the extent and duration of the intrusion, and whether the attacker came from inside or outside the company. Depending on the sophistication of the intruder, the case can be cracked in a few days or take years. Cases are routinely complex, and often involve international connections. The following cases serve as examples of typical cyber crimes:

**Raymond Torricelli, aka "rolex"**

Raymond Torricelli, aka "rolex," the head of a hacker group known as "#conflict," was convicted for, among other things, breaking into two computers owned and maintained by the National Aeronautics and Space Administration's Jet Propulsion Laboratory ("JPL"), located in Pasadena, California, and using one of those computers to host an Internet chat-room devoted to hacking.

Torricelli admitted that, in 1998, he was a computer hacker, and a member of a hacking organization known as "#conflict." Torricelli admitted that he used his personal computer to run programs designed to search the Internet, and seek out computers which were vulnerable to intrusion. Once such computers were located, Torricelli's computer obtained unauthorized access to the computers by uploading a program known as "rootkit." The file, "rootkit," is a program which, when run on computer, allows a hacker to gain complete access to all of a computer's functions without having been granted these privileges by the authorized users of that computer.

One of the computers Torricelli accessed was used by NASA to perform satellite design and mission analysis concerning future space missions, another was

used by JPL's Communications Ground Systems Section as an e-mail and internal web server. After gaining this unauthorized access to computers and loading "rootkit," Torricelli, under his alias "rolex," used many of the computers to host chat-room discussions.

Torricelli admitted that, in these discussions, he invited other chat participants to visit a website which enabled them to view pornographic images and that he earned 18 cents for each visit a person made to that website. Torricelli earned approximately $300-400 per week from this activity. Torricelli also pled guilty to intercepting usernames and passwords traversing the computer networks of a computer owned by San Jose State University. In addition, Torricelli pled guilty to possession of stolen passwords and usernames which he used to gain free Internet access, or to gain unauthorized access to still more computers. Torricelli admitted that when he obtained passwords which were encrypted, he would use a password cracking program known as"John-the-Ripper" to decrypt the passwords. He also pled guilty to possessing stolen credit card numbers that he obtained from other individuals and stored on his computer. Torricelli admitted that he used one such credit card number to purchase long distance telephone service.

Much of the evidence obtained against Torricelli was obtained through a search of his personal computer. In addition to thousands of stolen passwords and numerous credit card numbers, investigators found transcripts of chat-room discussions in which Torricelli and members of "#conflict" discussed, among other things, (1) breaking into other computers; (2) obtaining credit card numbers belonging to other persons and using those numbers to make unauthorized purchases; and (3) using their computers to electronically alter the results of the annual MTV Movie Awards. This case illustrates the wide variety of criminal acts which can result from security vulnerabilities.

**Raphael Gray, aka "Curador"**

On March 1, 2000, a computer hacker using the name "Curador" compromised several e-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and stole as many as 28,000 credit card numbers with losses estimated to be at least $3.5 million. Thousands of credit card numbers and expiration dates were posted to various Internet websites.. After an extensive investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (Wales, UK) Police Service in a search at the residence of "Curador," Raphael Gray. Mr. Gray, age 18, was arrested and charged in the UK along with a co-conspirator under the UK's Computer Misuse Act of 1990. This case illustrates the benefits of law enforcement and private industry

around the world working together in partnership on computer crime investigations.

**Bloomberg Extortion**

Kazakhstan citizens Oleg Zezov, and Igor Yarimaka were arrested on August 10, 2000 in London, England for breaking into Bloomberg L.P.'s Manhattan computer system in an attempt to extort money from Bloomberg. Zezov gained unauthorized access to the internal Bloomberg Computer System from computers located in Almaty, Kazakhstan. In the Spring of 1999, Bloomberg provided database services, via a system known as the "Open Bloomberg," to Kazkommerts Securities located in Almaty, Kazakhstan. Zezov was employed by Kazkommerts.

Zezov sent a number of e-mails to Michael Bloomberg, the founder and owner of Bloomberg, using the name "Alex," demanding that Bloomberg pay him $200,000 in exchange for providing information to Bloomberg concerning how Zezov was able to infiltrate Bloomberg's computer system. Michael Bloomberg sent e-mail to Zezov suggesting that they meet. Zezov demanded that Michael Bloomberg deposit $200,000 into an offshore account. Bloomberg established an account at Deutsche Bank in London and deposited $200,000. Michael Bloomberg suggested that they resolve the matter in London and Zezov agreed.

On August 6, 2000, Yarimaka and Zezov flew from Kazakhstan to London. On August 10, 2000, Yarimaka and Zezov met with officials from Bloomberg L.P., including Michael Bloomberg, and two London Metropolitan police officers, one posing as a Bloomberg L.P. executive and the other serving as a translator. At the meeting, Yarimaka allegedly claimed that he was a former Kazakhstan prosecutor and explained that he represented "Alex" and would handle the terms of payment. According to the Complaint, Yarimaka and Zezov reiterated their demands at the meeting. Shortly after the meeting Yarimaka and Zezov were arrested. On February 27, 2003, the trial of Anatoljevich Zezev concluded with a guilty verdict for computer fraud, extortion, use of interstate communications for extortion, and conspiracy. He faces a maximum of 28 years in prison. This case is an example of a traditional crime facilitated by a computer.

Cyber crime continues to grow at an alarming rate, and security vulnerabilities contribute to the problem. We encourage administrators and security professionals to reduce opportunities for criminals by employing best practices and patching vulnerabilities before they can be exploited. The FBI will continue to aggressively pursue cyber criminals as we strive to stay one step ahead of them in the cyber crime technology race.

I thank you for your invitation to speak to you today and on behalf of the FBI look forward to

working with you on this very important topic

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
Subcommittee on Consumer Credit
April 3, 2003

Madame Chairwoman, Mr. Chairman, thank you for the opportunity to testify before the Subcommittees. My name is Evan Hendricks, Editor & Publisher of Privacy Times, a Washington newsletter since 1981. For the past 23 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.

The three cases you have chosen serve as excellent illustrations of several privacy and security problems that are inherent when data on millions of individuals are maintained electronically in vast databases or data networks.

In summarizing some of the problems that enabled these data leakages, you will see why it is very likely there will be more leakages, and that the overall problem of the misuse of personal data will get worse before it gets better.

- While thousands of organizations have instant access to consumers' sensitive personal data, consumers do not have the same instant access to their own data. Therefore, they generally are unable to monitor when their data are accessed, by whom, and for what purpose.

- Except in California after July 1, 2003, organizations to my knowledge are not obligated by statute to inform record subjects that their personal information has been compromised.
- The over-reliance on the Social Security number as a personal identifier can increase the vulnerability of stored personal information, and, more importantly, increase its value once it is compromised.
- There is not a strong organizational culture of data security throughout many organizations, even though they maintain or have access to the personal data of millions of Americans. This is due in part to the relative "newness" of the electronic data age, but in my opinion, more attributable to the absence of law and policy that would require organizations to take seriously the issues of data security and privacy. In the Eli Lilly case, the Federal Trade Commission has taken an important first step on this front. But the three cases we discuss today demonstrate that much, much more needs to be done.
- Unlike most other Western countries, the United States lacks an independent enforcement office for privacy. In other countries, Privacy Commissioners (sometimes called Data Protection Commissioners) can investigate and/or audit organizational practices, and provide assistance to victims of data leakages.

Clearly, a central issue is the lack of transparency to consumers of what is happening to their personal data. This is one reason why the access issue is vital.

**Teledata Communications Inc (TCI)**

The facts of the TCI case have already been described by previous witnesses. More details are available at www.msnbc.com/news/839678.asp. In fact, to see how the problem of credit fraud and data leakages consistently has worsened over the past five years, one only needs to do a search at msnbc.com under the name of Bob Sullivan, to see his excellent reporting on numerous cases.

TCI is a classic case of some of the problems I described above, including incredibly lax security in a credit bureau environment in which the data of 200 million Americans are at risk, and, 30,000 consumers that did not have a clue their data was misused until they received nasty calls from debt collectors or were rejected for a loan based on an inaccurate, polluted credit report.

What's stunning about TCI is that it continued for three years, allegedly perpetrated by a ring led by a 10-month employee, Philip Cummings. Security for

passwords was so lax that Cummings was able to electronically masquerade as Ford Motor Co. and other major companies, pull credit reports in their names, and sell the data to a Nigerian fraud ring. Even after Cummings left TCI and move out-of-state, he was able to continue using passwords that allowed him, from February to May 2002, to pull 6,000 reports, 100 at a time, in the name of Washington Mutual Bank. And as recently as September 2002, long after the Ford Motor incident had been well-publicized, the Cummings ring ordered 4,500 credit reports through Central Texas Energy Supply.

When a company did change its password, temporarily stumping the laptop on which Cummings had downloaded passwords and given to another ring member, the ring member, who is now cooperating with prosecutors, claimed he just called Cummings, who had an ample list of additional passwords that still worked.

The result was some 30,000 individuals having their good names used for fraud, with initial losses pegged at $2.7 million and rising fast. Those individuals all must endure the nightmare of being blindsided by identity theft, which includes the time-consuming, emotional distressful process of cleaning up a polluted credit report and restoring their good names.

This is where the issue of access is important. If individuals were "plugged into" their credit reports, they could receive alerts via e-mail of activity on their credit report. Upon seeing that, say, Texas Energy Supply, pulled their report, they would immediately know that something was wrong and take action. In fact, the three major credit bureaus (CRAs) are selling electronic access and alert services to consumers. But they generally charge in the $60-80 range, meaning it would cost a consumer around $200 to get the service from all three bureaus. In my opinion, this is an excessive charge, considering that consumers are seeking information about themselves. The Fair Credit Reporting Act caps the price CRAs can charge for credit reports, but does not address excessive charges for the relatively new monitoring services. The more we can encourage American to be plugged into their credit reports and other personal data, the better we will be able to combat the kinds of problems that we are discussing here today. Meanwhile, CRAs look at their credit monitoring and alert services as a potentially major revenue stream.

The TCI case also illustrates a shocking lack of security and vigilance on the part of the credit bureaus. For three years, the Cummings gang ran what appeared to be a readily discernible pattern of wholesale ripoffs of thousands of confidential

credit reports. Yet throughout that period it appears that none of the CRAs had a monitoring or audit system to spot this suspicious pattern of activity. It's widely known and accepted that credit card companies use software to monitor suspicious buying patterns as a means of flagging stolen credit card use. This protects both the consumer and the credit card company. But the TCI case, and my own experience, suggests that CRAs have not used similar systems to flag suspicious activities.

Finally, because this was a criminal case prosecuted by the U.S. Attorney, the U.S. Attorney attempted to notify the 30,000 victims. In my opinion, because their lax security was the cause of this problem, TCI and the CRAs, not the American taxpayer, should have borne the cost of notifying victims. Conversely, i this had not become a criminal case, would individuals have been notified? Did the CRAs notify victims after their credit reports were pulled in the highly publicized Ford Motor incident?

**TriWest Break-In**

The TriWest break-in remains a mystery. Although promising frequent updates on the case when it first became public, TriWest has not posted an update since February 2, 2003. Federal authorities reportedly are investigating. TriWest said computer containing incredibly sensitive medical claims history was stolen from a "secure room." To its credit, TriWest said it attempted to notify beneficiaries by sending them letters and by posting notices on the Web site. Moreover, the TriWest Web site now creates a pop-up ad that easily allows beneficiaries to place a "fraud alert" on their credit report.

TriWest illustrates how an organization that had every reason to take reasonable steps to safeguard data security, didn't. A major part of this is the organization's decision to use the SSN as a personal identifier, which increases the value of the stolen data and the risk to individuals.

As a DOD contractor, TriWest presumably must comply with the Privacy Act. One of the Act's requirements:

> "Agencies must establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm,

> embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

Moreover, TriWest was handling very sensitive medical information deserving a high level of protection. To leave it in database without encrypting it or other protective measures is, in my opinion, inexplicable, particularly in light of the Privacy Act's reference to "anticipated threats."

Also highly questionable is the reliance on the SSN as an identifier. Like many health care providers, TriWest is neither required nor prohibited from using the SSN, but insists on using it. This raises the risk level, because the SSN is one of the first pieces of information coveted by an identity thief. Meanwhile, America's fighting troops are at great risk because nearly all of their military records are tied to the SSN.

Hopefully, pending litigation will shed important light on the details of the TriWest case.

**DPI Merchant Services**

Another case shrouded in mystery is the theft of more than 10 million Visa, MasterCard and American Express Card numbers via DPI Merchant Services, a credit card processor. When the story first was reported, Visa and Mastercard initially declined to disclose which credit card processor had been hit. Then when DPI's role was revealed, no one would reveal which banks were affected. As you'll see from the following story from the March 3 edition of *Privacy Times*, Visa fined someone, something, but wouldn't say who or what. There was also a conscious policy by many of the entities involved not to inform cardholders that their credit card numbers had been compromised.

> The firm, also known as DPI Merchant Services, said that there still was no sign of fraudulent use of the stolen credit card numbers. According to news reports, Citizens Financial Bank of Providence, R.I., closed 8,800 accounts and sent customers new cards. PNC Bank said 16,000 debit cards were exposed. However, the vast majority of cardholders apparently have not been informed, and there has not been a complete disclosure of which issuing banks were affected. DPI's parent company, TransFirst Corp., said in one press release that it services 450 community banks.

> DPI told the *Detroit News* that consumers who are concerned should contact the issuing banks. However, N. Scott Jones, a DPI spokesman, declined to identify which banks had been hit. "That's not our call – it's the Associations'," he said referring to Visa and MasterCard. Both organizations already had notified the affected banks, he added.
>
> At 11:00 pm (EST), Friday, Feb. 28, Visa posted a statement at www.businesswire.com that, "In relation to the unauthorized intrusion that occurred in early February, Visa USA has levied substantial fines in this matter. We will take whatever further action is necessary to safeguard Visa cardholders. Visa continues to monitor the potentially compromised accounts, however, to date there has been no fraudulent activity. While we must respect the sensitive nature of this ongoing investigation, it is important for Visa cardholders to know they are fully protected by Visa's $0 liability policy, which means they pay nothing in the event of unauthorized purchases." Visa declined to release more details, stating that it never names banks whose security has been compromised or entities that it has fined.
>
> Jones downplayed the importance of further disclosure, stating that it would be difficult to misuse stolen credit card numbers and expiration dates without the cardholder's name and address, and without the three-digit security number on the back of the card. He said no other personal information about cardholders was compromised.

It's my firm belief that when there are security breaches of personal data, national policy and organizational practice should generally require that individuals be notified. In most other contexts, if authorities known that someone is a victim of a crime, the victim is notified. As with nearly all privacy issues, reasonableness standard must be applied case-by-case as to when notice is required, as well as to the means of delivering notice. But there should be no escaping the fundamental premise that people have a right to know when organizational negligence has exposed their personal data to serious risk. Unfortunately, the DPI case shows this is clearly not the standard adhered to by some leading financial institutions.

A California law that takes effect July 1, 2003 is the first to require such notification. Below is a description of the new law.

> A new law in California requires state agencies and businesses that own databases to disclose security breaches involving certain personal information. The bill comes in response to an April 2002 incident in which the records of over 200,000 state employees were accessed by a computer cracker. The California legislation exceeds federal protections, as there is no national requirement for notice to individuals when personal information is accessed without authorization.

> Senate Bill 1386, sponsored by Senator Steve Peace (D-El Cajon), creates a notice requirement where there has been an unauthorized acquisition of an individual's name along with a Social Security Number, a driver's license number, or an account number and corresponding access code. The notice requirement is also triggered when there is a reasonable belief that a security breach occurred. Notice must be given "in the most expedient time," but may be delayed where it would impede a criminal investigation.
>
> The law requires notice to be given to individuals in writing or electronically, in accordance with federal e-signature law. If the cost of notice were to exceed $250,000, or where over 500,000 people were affected by the security breach, notice could be delivered through a combination of e-mail, a conspicuous posting on the agency or company Web site, and notification of statewide media outlets. Agencies and companies could also create information security policies in advance of security breaches to address the notice requirement.
>
> The law does not apply to non-computerized files, such as personal data stored on paper. Also, only California residents enjoy the law's protections. Californians can bring civil actions for damages and injunctive relief against entities that fail to comply with the law. The law takes effect on July 1, 2003.

This also illustrates why Congress should be very, very cautious about preempting State law in the area of privacy or data security. In the past few years, at a time when these issues are increasing in importance, Congress generally has not demonstrated that it is capable of enacting adequate privacy and security protections for consumers. However, the States continue to respond more quickly with innovative legislative approaches that have helped improve organizational practice nationwide.

Finally, a sidebar issue is that the technology exists so that credit cards, instead of relying on a constant payment number that is vulnerable whenever stored, could issue one-time or "disposable" numbers that would be good for only one transaction. However, the credit industry has declined to invest in this technology.

**Identity Theft Will Worsen As Well**

A new report by the Tower Group confirms losses from identity theft are growing, but effectively predicts the problem will worsen. Although pegging identity theft losses at $1 billion a year and rising, a financial analyst does not foresee any major near-term changes in the practices of financial institutions.

Christine Pratt, the author of the report and a senior analyst in TowerGroup's consumer credit practice, said losses still only constitute a fraction of overall revenues, and financial institutions benefit more by offering easy and quick credit than they are hurt by losses stemming from identity theft.

"Nobody has taken a huge hit yet. And there are not a lot of easy ways to tighten up controls without putting yourself at a competitive disadvantage. Almost no one thinks the consumer is willing to give up much of anything to prevent ID theft," Pratt said.

**Conclusions & Recommendations**

These are complex and serious issues. Unfortunately they promise to worsen for many of the reasons I've described above.

Here are some of my preliminary recommendations:

- **Expand & Improve Consumer Access to Their Own Financial Data**. The FCRA already gives consumers the right to see their credit report and caps how much CRAs can charge. This approach needs to be upgraded to the electronic age and expanded to the entire realm of financial data, especially since large financial institutions are maintaining their profiles on customers, perhaps beyond the reach of the FCRA. In the meantime, Congress could pass a Resolution or Sense of the Congress that as a matter of principle and fundamental fairness, Americans should have a right to see and correct information about themselves.

- **Extend to financial institutions the following security standard** that federal agencies must abide by under the Privacy Act: "Agencies must establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Again, this goal could be advanced in the interim through a resolution or Sense of the Congress.

- **Impose A General Duty To Notify Consumers After Data Leakages.** The new California law provides a model starting point.

- **Curtail The Use of SSNs as a personal identifier**. Rep. Clay Shaw and others have introduced legislative proposals to this effect.

- **Create An Independent Privacy Office** Most people don't realize that Sen. Sam Ervin originally proposed such an office along with the Privacy Act. Now, every advanced nation has one except the United States.

- **Create A Private Right Action So People Can Enforce Their Own Rights**. Privacy affects virtually all 200 million adult Americans. In this electronic age, they must have rights, and those rights must be enforceable. You will never be able to build a bureaucracy big enough to adequately enforce Americans' right to privacy, nor should you want to. Thus, the private right of action is essential.

I'd be happy to answer any questions.

# Written Testimony of

**David J. McIntyre, Jr.**
**President and CEO**
**TriWest Healthcare Alliance**

**Before the**

**U.S. House of Representatives Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit and the Subcommittee on Oversight and Investigation**

**April 3, 2003**

**Introduction**

Chairwoman Kelly, Chairman Bachus and distinguished members of the Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit and the Subcommittee on Oversight and Investigations, I would like to thank you for the invitation to appear before you today to discuss the important topic of identity theft. Unfortunately, this is becoming an increasingly prevalent issue and as consumers we are all concerned. I would like to thank you for the focus you are giving this critical issue and for your desire to enhance safeguards for consumers. In fact, as I have come to learn, many of you have been focused for some time on enhancing consumer protection against identity theft.

My name is David McIntyre. I am the President and CEO of TriWest Healthcare Alliance, a private corporation that administers the Department of Defense's (DoD's) TRICARE program in the 16-state Central Region. We are the largest Department of Defense contractor based in the state of Arizona and are privileged to serve the health care needs of those who have or currently defend our freedom and their families. In mid-December, our company was the victim of a theft that has placed at risk the personal information of more than a half-million current and former TriWest customers (TRICARE beneficiaries), many of whom are also our employees.

Identity theft is a serious federal crime that affects more and more Americans each year. In fact, this crime victimized nearly 1 million Americans last year alone. This crime causes billions of dollars of harm to Americans each year. The thieves who commit these crimes against consumers don't just acquire merchandise illegally or use fake identification to obtain anything from a driver's license to a job; they wreak havoc on the lives of their victims. Repairing the damage done to a victim's credit record is costly and time-consuming. In fact, it often takes years for a victim of identity theft to clear up the mess created, and sometimes, their credit is permanently ruined.

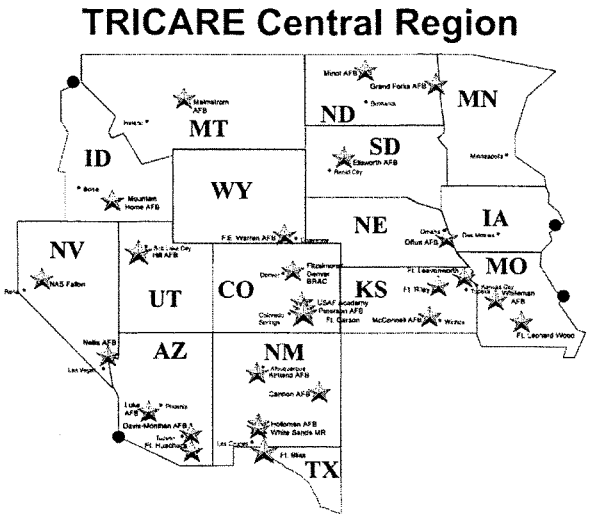
In my opinion, there are few consumer issues more worthy of the attention of your Committee than this topic. And, on behalf of TriWest's employees and those we serve, I would like to commend you for your focus on this rapidly growing crime and the importance you are placing on the need for action. I am hopeful that your efforts will be successful and that they serve to enhance protection for America's consumers from this insidious crime. Accordingly, I am pleased to be here today to share the details of our story and some thoughts I have about action that could be taken to protect consumers.

I am particularly honored today to be in the presence of two of Arizona's Congressmen, John Shadegg from Arizona's 3rd District and Rick Renzi from Arizona's 1st District. I applaud their leadership on this critical consumer issue, particularly that of Congressman Shadegg who first started working on this issue 6 years ago, in response to the troubling experience of one of his constituents.

**TriWest Healthcare Alliance and the TRICARE Central Region Beneficiaries**

TriWest is the Managed Care Support Contractor for the TRICARE Central Region. We partner with the military to meet the health care needs of more than 1.1 million members of our nation's military family (active duty, their families, and retirees and their family members).

Based in Phoenix, Arizona, we have remote office locations across our Central Region. Most of our offices are on military installations.




● Areas not included in the TRICARE Central Region: Yuma, Ariz., contained in Region 10; six northern counties in Idaho contained in Region 11; certain ZIP codes in the St. Louis, Mo.area, and the Rock Island Arsenal area in Iowa, contained in Region 5.

TriWest has a strong history of collaboration and partnering with our military/ government counterparts in the Central Region. In addition, we remain steadfastly amenable to providing information to the DoD, Congress, and Committees such as these, to the benefit of the TRICARE program overall, as well as the deserving population we serve.

**Computer Theft at TriWest's Secondary Corporate Office**

On Saturday morning, December 14, our secondary corporate office in Phoenix, AZ, was burglarized. Computer equipment and data files containing confidential and personal files of more than 500,000 members of America's military family were stolen from the premises. The information included on the stolen hard drives includes names, addresses and Social Security numbers, along with other personal information.

The burglary was discovered on December 16. Since that day, TriWest has coordinated closely with the authorities who are conducting the criminal investigation.

Presently, the identity of those who committed this crime and the motives behind the crime are still unknown. While information has been compromised, we do not have any verification that anyone's personal information has been misused or will be misused. The very possibility, however, that it could be misused called for prompt action on our part to inform our customers about the compromising of their personal information and education about the steps they can take to protect themselves.

**Coordinated DoD/TriWest Response to the Theft**

From the day we discovered the theft, we began coordinating with our DoD partners. Once we had compiled the list of affected individuals from our backup tapes, we began working around the clock with the leadership of the DoD and the Military Health System to create and implement a comprehensive communication plan to protect our beneficiaries.

The plan employed a three-prong approach that began with TriWest contacting the media to broadcast news of the theft and stress the need for individuals to protect themselves. Second, the DoD, working through the military commands, disseminated information to every installation, worldwide. The third component of the communication plan included a letter campaign that contacted every beneficiary affected by the theft, and which included information on steps they could take to protect themselves against misuse of their personal information.

The execution of this communication plan is now complete.

I would like to share with you, in detail, the specifics of our efforts; however, I would like to first express my deep personal gratitude to the DoD for responding to this issue, and to Dr. Bill Winkenwerder, the Assistant Secretary of Defense for Health Affairs, for the immediate attention he gave the theft and the invaluable leadership he provided as we worked side-by-side with the other components of the Military Health System to deal with the situation. Without this coordinated response, our efforts to inform those impacted by the theft would not have been as successful.

For the past three months, this issue has been a critical focus for our company. First and foremost, we believed it was necessary to alert the DoD, as well as the affected

individuals, so that they could take action to protect themselves, should the thieves choose to misuse the personal information they illegally obtained. The following is a detailed account of the activities we were engaged in as a result of the theft. These include our ongoing efforts and reflect our continued commitment to respond quickly and aggressively to this issue:

- Authorities were contacted; federal investigators worked to find the individual(s) responsible for the crime.
- TMA and SAIC personnel analyzed what, if any, additional security measures should be taken to protect TriWest from another theft.
- The DoD began working with TriWest to ensure an uninterrupted delivery of medical benefits.
- I personally called the 23 beneficiaries whose credit card information was stolen. Information regarding the theft was conveyed, and the beneficiaries were encouraged to take action to protect themselves from the misuse of their credit card. The beneficiaries were also provided contact information in the event they encounter any suspicious activity with their credit card.
- TriWest's proposed communication plan and messages were delivered to the Office of the Secretary of Defense (OSD) for review.
- A memo was distributed to all TriWest employees via email. Additional security policies were also distributed to all employees.
- The strategy for communicating the issue to beneficiaries was completed (with OSD approval).
- Ongoing communication updates were provided to TriWest's Board of Directors and subcontractors.
- Designated TriWest customer service personnel were trained to staff dedicated phone lines for incoming beneficiary calls.
- TriWest communicated with key Congressional leadership, Beneficiary Associations, and affected providers.
- Dr. Jerry Sanders, TriWest's Vice President of Medical Affairs and retired Deputy Surgeon General of the Air Force, personally contacted active and retired General Officers to inform them of the theft and our communication plan.

The communication strategy continued to be implemented throughout the holidays. By the end of December, TriWest had contacted each of the potentially affected individuals or families, and had also built a unique e-mail system, a web site and a call center to provide information and answer questions beneficiaries may have about the identity theft issue as well as the safeguards they can take to protect themselves. In addition, TriWest coordinated with the three credit bureaus to provide information on how to combat identity theft and place fraud alerts in their individual credit files.

Since the discovery of the theft, we at TriWest have taken measures to reconfigure our systems and enhance our security. In addition, we have been working with federal personnel and a top private sector information security company to review all aspects of our physical and data security in an attempt to make sure that we understand all of the actions we should take to minimize the chance that such an event is repeated.

As a result of the break-in at our secondary corporate facility, we have learned a great deal about the issue of identity theft; it quickly became apparent to us how difficult it can be to catch those who commit such crimes. Therefore, TriWest posted a $100,000 reward in the hopes of assisting local and federal law enforcement to obtain information leading to the arrest and successful prosecution of those responsible for this very serious federal crime -- a crime affecting more than 500,000 of our nation's patriots. I remain hopeful that the $100,000 reward that TriWest posted will encourage anyone that might know something to come forward and inform the authorities about the people responsible for this crime and the location of the stolen information.

**Invaluable Lessons Learned**

The theft of this computer equipment and the files contained within is a matter of grave concern to everyone at TriWest as well as the DoD. As a result of the theft, and because it is the right thing to do, we have become a more security-conscious organization.

We have conducted a thorough security vulnerability assessment, taken action to improve security across the enterprise, and, while there is more work still to be done, we are confident we have contained further significant threats to our beneficiaries' personal information.

However, we will never become complacent with respect to maintaining the privacy of our beneficiaries.

The following are some of the steps we have taken to make sure nothing similar to this event happens within our organization again.

- TriWest has built an information technology infrastructure that includes enhanced security features. We have also hired an interim Chief Information Office, retired Navy Rear Admiral Todd Fisher.
- TriWest has established a Security Steering Group with responsibilities to oversee data and physical security policies and practices throughout our corporation. The Security Steering Group reports directly to me as President and CEO. Specific duties of the Group include:
    - Oversight of the IT security management program;
    - Oversight of the execution of the company's Facility Security Plan; and
    - Human Resources actions to include access privileges, background checks, and other classification actions including security awareness training for all personnel.
- TriWest has upgraded its incident reporting system.
- TriWest has received initial authority as part of the DoD's DITSCAP requirements (the DoD's security certification and accreditation process) and exceeded some implementation requirements by employing state-of-the-art security procedures.

**Challenges We Have Encountered and the Positive Results We Have Achieved**

TriWest researched information published by the Social Security and Federal Trade Commission (FTC) relating to information and identity theft. We developed a white paper, "Safeguard Yourself," as well as a telephone call center script that was based on the information we'd gathered. The paper included a description of the process our beneficiaries should employ to determine whether they are a victim of information or identity theft; how to initiate the placement of a fraud alert on their credit records; and how to contact each of the three credit bureaus in the United States. We submitted the paper to the attorneys in the FTC department that oversees identity theft and requested their review and suggested edits. They were extremely cooperative and helpful in reviewing the information we planned to provide our beneficiaries.

Following the review of our paper, one of the FTC attorneys, Naomi Lefkovitz, provided us with suggested contact points at each of the credit bureaus. We called each one to advise them of our situation and to seek their assistance and advice. They reported that the calls related to our theft caused a 300–400% increase in calls to their call centers.

A review of the calls received by our own Theft Hotline indicated that beneficiaries were asking whether TriWest could initiate the fraud alert with the credit bureaus on their behalf. This issue was a point of discussion between TriWest and the DoD; determination was made by the DoD Privacy Officer that, with permission of the person involved, we could initiate the fraud alert on their behalf.

Hence, discussions were held with each of the credit bureaus. TransUnion and Equifax agreed to accept requests, consistent with Privacy Act requirements, from us on behalf of beneficiaries. TriWest developed a plan that allowed beneficiaries to complete a request and authorization form on our web site, which was then transmitted to the credit bureau for their action. This process was implemented in an encrypted, secure manner. Experian determined that they would establish a web-based request for Fraud Alerts and an online viewing of the consumer's credit report. It was their preference for the consumer to enter their request directly into Experian's system via a hotlink from TriWest's web site.

Each of the credit bureau representatives noted that this was the first arrangement of this nature by their organizations on behalf of consumers.

This process is still in place. Upon receipt of the request and identifying information, the credit bureaus send a letter of notification regarding the fraud alert to the beneficiary, along with a copy of their credit report. (These arrangements were all made at no cost to the individual beneficiary.) The web request for fraud alerts was activated at the end of January 2003; since that time, over 63,000 beneficiaries have initiated fraud alerts.

Development of the web process for fraud alert requests made the process much more convenient for beneficiaries. By accepting batches of data files rather than thousands of

calls to their call centers, it also served as a means of cost avoidance for the credit bureaus' call center operating costs. The credit bureaus have been exceptionally helpful and responsive throughout this entire process, on both the technical and executive levels. Their advice, assistance, and cooperation have been noteworthy and extremely valuable.

Without a doubt, we must rein in identity theft. Again, that is why I am so appreciative of the focus that this Committee and its relevant Subcommittees are giving this issue. Companies and consumers must take more aggressive steps to combat this crime and protect themselves. Based on all I have learned these past weeks, I would suggest three additional measures.

First, any organizational leader, be they public or private, whose organization suffers the theft of customers' personal information has an absolute obligation to inform those customers of such an event and help them understand what they can do to protect themselves against the misuse of that information. I understand personally the difficulty, cost and awkward nature of such disclosure, but to do anything less is wrong.

After all, we are merely stewards of our customers' personal information as we seek to serve their needs. This is not our information; it belongs to our customers. And to not inform them of such an event for fear that we would lose their confidence or subject our company to negative publicity is unacceptable. It places our customers at even greater risk by preventing them from taking steps to protect themselves.

The safeguards that consumers can take to shield themselves from fraudulent uses of their personal information are uncomplicated and, if accomplished quickly enough after the theft, quite effective. Quick and decisive actions such as flagging your credit file, notifying your bank and other major creditors to watch for unusual activity and contacting the Federal Trade Commission to file a complaint can save years of expensive and time-consuming effort for consumers affected by such thefts.

Second, as a consumer, I've observed the inconsistencies in how credit card numbers/accounts are handled among merchants. Specifically, I have noticed the variance in how credit card numbers are displayed on receipts. For instance, some receipts include the entire credit card number, expiration date and full name of the cardholder, which means the card number can now be used by anyone who happens to pick up the receipt. Other receipt slips contain only the last four digits of the credit card number, which offers more protection against misuse of the account.

I believe that standardization of how credit card numbers are displayed on receipts, to block out most of the numbers, is one more way in which Americans could be better protected against identity theft, as it would help to minimize this type of criminal activity.

And third, I believe the federal penalties for identity theft offer little deterrent to those bent on committing such a serious crime. For example, I was appalled to learn that the maximum federal penalty for such crimes is five years in prison and a $250,000 fine.

These penalties must be significantly increased to serve both as an effective deterrent and a sufficient punishment.

During the 107th Congress, lawmakers introduced more than two dozen bills to thwart identity theft and assist victims. Unfortunately, none of them made it into law.

I hope that the 108th Congress will be able to muster the support to move legislation in this area – strengthen the laws used to deal with those who perpetrate such crimes and enhance the protections for Americans.

Without question, the process of changing our laws is difficult. Our system of government requires careful deliberation, and that takes time. But thieves don't have to wait for public debate. They utilize new technologies as soon as they figure out how to profit from them. As a result, laws often play catch-up to technology. And, as our case and the others you will be hearing about today suggest, the criminals unfortunately have the upper hand.

Federal and state laws have yet to be tightened to provide law enforcement with effective enough tools to aggressively deal with the onslaught of identity theft. Unfortunately, in the breach lies the consumer. Identity thieves know that if they are caught, the punishment and penalties are a fraction of those for robbing a bank. Yet, the financial impact of the crime can be much greater.

It is my hope that Congress will champion the cause of strengthening penalties that predate the information age and take steps to modify the rules in the credit industry to add an effective layer of protection.

**Conclusion**

In an effort to protect our customers, we have dealt aggressively with this issue. We have communicated with all of the affected parties and the government. In addition, we have shared this experience and the lessons learned with all of the Department of Defense Health System's contractors and the direct care system.

The criminal investigation remains active, led by the Defense Criminal Investigative Service and supported by the U.S. Attorney in Phoenix, the Federal Bureau of Investigation, and other law enforcement agencies.

We have been commended for our response to the theft and our honesty and openness in communicating with those whose personal information was put at risk. In fact, we have received many words of praise from our beneficiaries. Of note, General Myers, Chairman of the Joint Chiefs of Staff, a former beneficiary of ours, whose name was included in the stolen data files, sent us a letter to applaud us for our immediate and responsive actions to the situation. While we appreciate the praise, all we did was respond by doing the right

thing by our customers who were infringed upon and whose financial integrity was placed at risk due to the burglary we suffered.

TriWest Healthcare Alliance takes great pride in the work that we perform. It is a privilege and a pleasure to support the Military Health System and the beneficiaries of the current TRICARE Central Region. These are the very individuals who have or are currently putting their lives on the line for freedom.

I am grateful that your Committee and its Subcommittees are focused on this very important topic. The commitment you are making to learn more about identity theft and take a proactive stance against its rampant spread is not only admirable but is also the bridge that is needed to make the public more aware of the potential every American is susceptible to, while sending a message to the criminals who perpetrate such insidious crimes. I would like to thank you for the opportunity to share this experience with you and provide information to you on this critically important topic.

Thank you for the invitation to participate in today's hearing. I would be glad to answer any questions that you might have of me.

Kevin Mitnick

Testimony Before the House Financial Services Committee

"Fighting Fraud: Improving Information Security"

April 3, 2003

Chairwoman Kelly, Chairman Bachus, and distinguished Members of the Committee —

My name is Kevin Mitnick. I appear before you today to discuss your efforts to review current industry practices concerning security procedures for the prevention of electronic theft of credit-card information. My understanding is that you are examining how to coordinate efforts among law enforcement, credit issuers, credit bureaus, and third-party vendors that process transactions, to limit harm to consumers and businesses when data security is breached.

I am primarily self-taught. My hobby as an adolescent consisted of studying methods, tactics, and strategies for circumventing computer security, and for learning more about how computer systems and telecommunication systems work.

I have 15 years experience circumventing information security measures, and can report that I have successfully compromised all systems that I targeted for unauthorized access, save one.

I also have two years experience as a private investigator, with responsibilities that included locating people and their assets using social engineering techniques.

I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed. I have used both technical and non-technical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings.

Currently I am the co-founder of Defensive Thinking, a Los Angeles-based information security firm. I recently co-authored with William Simon a book titled *The Art of Deception*, published by John Wiley and Sons, which has become an international bestseller. The book details non-technical methods and tactics — in essence, con-man techniques — that computer intruders use to compromise valuable information assets. The book also presents defensive techniques that companies and government agencies can employ to mitigate the risk of these so-called "social engineering" attacks.

Social engineering is a method where the intruder deceives his target into complying with a request based on false pretenses and psychological

manipulation. It is important to understand — and all companies and their employees need to realize — that the most insidious vulnerability to information security are the well-meaning, hard-working folks that use, operate, and maintain information systems.

The prevention and detection of social engineering attacks should not be ignored or underestimated. In fact, the majority of scams involving identity theft and credit fraud include social engineering on some level.

For instance, a thief can set up a phony eCommerce site by duplicating the real Web site of a Nike or a WalMart, and offer the products or services at what appear to be substantial discounts. The thief is then able to steer unsuspecting online shoppers to his phony site, where they enter their credit card numbers and other personal information to authenticate their purchases. The insider's term for stealing credit card information is "carding." After setting up his phony site, the "carder" then sits back and collects the credit-card information that pours in.

Another method that credit card thieves use to obtain private financial information is to send a phony instant message or forged email message that purports to be from the target's Internet Service Provider or an eCommerce site. The message explains that some kind of problem has occurred, and requests the user to provide his or her login name and password, or to reveal financial information.

In an attempt to deter carding, many retailers are now requiring an online customer to provide the three-digit CVC number that card issuers have begun to use. But the thief also asks for this CVC number. With it, he is able to use the information to commit fraud against an unsuspecting cardholder and the merchants.

In my previous testimony before the Committee on Governmental Affairs in March of 2000, I detailed the common vulnerabilities exploited to gain unauthorized access to information assets or computing resources. I recommended several risk mitigation strategies to increase the effectiveness of future security and reliability of information systems owned and operated by, or on behalf of, the federal government.

At the time, my testimony focused on the vulnerabilities of Federal computer systems — but these same vulnerabilities also exist throughout the private sector.

As you probably already know, identity theft and credit-card fraud are the fastest growing crimes of the decade.

I understand that the subcommittee will be examining three recent cases involving large-scale thefts of non-public personal identifying information and credit card details. A major part of the problem is that the criminals only needed to obtain information that is stored or processed in thousands of computer systems. You will learn that the methods they used varied from low-tech

skimming of cards by unscrupulous employees, to circumventing complex security measures at sites that store or process credit card information.

In February, 2003, DPI, a credit card processing services company, reported that an unknown intruder had compromised their network and gained access to a database that held over eight million credit card accounts. DPI did not release any details describing how the breach occurred, citing cooperation with Federal law enforcement officials.

The DPI case was widely reported in the press because of the astounding number of credit cards potentially compromised. But when examined closer, you will realize that these types of attacks happen all the time.

Subsequent to the DPI incident, computer intruders compromised a Georgia Tech computer system and obtained access to 57,000 credit card numbers.

In my opinion the committee should not overlook that many similar attacks on networks containing financial information are not detected by the owner or operator. It is important to realize that many of these security incidents remain undetected because of poor security and auditing practices.

DPI has publicly claimed that the intrusion occurred from outside the organization. Although I don't like to hypothesize on facts and circumstances of any attack without details, I would recommend that DPI consider the possibility that the attacker had assistance from the inside of the company.

Based on my experience, I would say that the attackers were able to exploit a technical vulnerability in the operating system or a particular service that was available to attacker via the Internet.

Every day the security community announces new vulnerabilities in operating systems and application software that have just been identified. Vulnerabilities in software can be exploited to gain remote access to the target computer. Many system programs contain programming errors that enable the intruder to trick the software into behaving in a way other than that which is intended in order to gain unauthorized access rights, even when the application is a part of the operating system of the computer.

Once a new vulnerability is recognized, the software developer or a security company develops a "patch" — a modification to the software — that must then be installed by individual companies, a process that may be overlooked for days, weeks, or even months. Meanwhile companies using that software remain vulnerable, or are forced to disable or block access to the vulnerable service until the patch becomes available.

Even then, in many cases, this is not enough. There are any number of sophisticated hackers who are able to discover previously unrecognized security vulnerabilities, and then use them to compromise computer systems and networks.

As a point of information — the programming instructions to exploit a new vulnerability may be well known to hackers, but the software manufacturer has not been notified of the problem.

This type of crime will continue to be attractive to electronic criminals as long as credit-card details are stored by businesses connected to the Internet.

I agree that it is essential to implement security strategies to prevent, detect, and respond to security threats and attacks. But it's too easy to look in the wrong direction for an answer. In my view, attempting to solve the complex problem by micro-managing every online site that accepts credit card transactions would turn out to be a wasteful, inefficient, and not a very successful exercise.

Instead, I recommend that the committee look in a different direction. I recommend that you explore mitigation strategies which focus on improving the authentication of the credit card user.

The challenge is a good deal easier when the customer is standing in a brick-and-mortar retail outlet with his or her credit card in hand. In this kind of face-to-face situation, mitigating fraudulent transactions may be achieved by assigning every credit card holder a personal identification code — one that is not printed on the credit card itself. This provides a two-factor form of authentication that is harder to circumvent as compared to merely depending on the possession of the physical card.

But this solution would not eliminate problems with online transactions, the situation that the credit-card industry refers to by the curious term "Card Not Present" — meaning that the cardholder is not face-to-face with a retail clerk or the like. In any online credit-card transaction, identity and authorization is based on the information a consumer provides to the merchant. This is no better than a static password. There's an old saying among hackers: "You never know if someone else has your password." The reality is that a password or its equivalent is too easy to steal.

A first step toward a solution would be to strip away the identity value of all personal information. If knowledge of a credit card number, expiration date, and the corresponding customer name and address is without value, stealing this information would be useless to an imposter. Unfortunately, authentication technology has not yet matured to the point of being able to provide a solution to this issue.

But the process of requiring another authentication factor would add cost to the entire infrastructure of business and would result in loss of sales due to consumer inconvenience. If not being done already, I would recommend that the industry explore using additional authentication practices that may include digital certificates; identification of the user's location based on IP address or telephone number; or verification of a PIN through another communication channel. For example, consider this scenario: You've just placed an Internet order for a new

cell phone with a price tag of several hundred dollars, and placed an online order with your credit card information. But you were not required to give a PIN number. Instead, you next dial your credit-card company, and when prompted, enter your card number. An automated system then reads off details of the transaction. You are satisfied that the details are correct. The system then tells you, "To authorize this transaction, enter your PIN number."

This process would probably be used only for more expensive Internet purchases, since it does require an extra step by the consumer and additional cost to the credit-card companies for handling the authorization phone calls.

What would be the advantage of this approach? The thousands upon thousands of individual retailers would not have access to consumer PIN numbers. The fact that so many retailers store the credit-card numbers of online customers gives rise to the kind of card-number theft that this hearing is addressing. If they also store the customer's PINs, then there's no gain in security — the PIN becomes almost worthless as a security element.

But under the approach I've suggested, only the card issuer would have access to the PIN-number information. Under this arrangement, theft of the card numbers would be of limited value. Using a card for many fifty-dollar purchases makes the bad-guy more susceptible to identification and arrest.

In another area, I also recommend consumer awareness training programs that educate people about the various scams being used to steal their credit card details and personal information, a practice that can prove highly valuable to effectively minimize identity theft and credit card fraud.

So I respectfully submit for your consideration these recommendations for the improved security of online retail transactions and credit-card protection against theft and fraud. I believe that all online retailers who accept credit card should be encouraged or required to do the following —

1) Perform a regular, thorough risk assessment of their information assets, especially systems that process or store consumer financial and personal information.

2) Implement policies, procedures, standards and guidelines as dictated by the results of the risk assessment.

3) Create an audit and oversight program that measures compliance. The frequency of the audits ought to be determined consistent with the mission; the more valuable the data, the more frequent the audit process.

4) Develop a process to insure meaningful and effective patch and configuration management for all computer systems.

5) Employ authentication methods that do not use non-public personal identification information such as mother's maiden name, birth date, birth

place, driver's license number, address, phone number, or social security number.

6) Effective audit procedures -- implemented from the top down – must be part of an appropriate system of rewards and consequences in order to motivate system administrators, personnel managers, and employees to maintain effective information security consistent with the goals of this committee.

7) Establish a security awareness training program designed to educate their employees on threats to information security, and to change employee behavior to foster a secure environment. These would follow security recommendations described in detail in my book *The Art of Deception.*

In terms of legislation, I recommend that the subcommittee consider the following:

1) Legislation that prohibits merchants or credit card processors from electronically storing PINs or other types of verification credentials such as CVC and CVC2, unless essential to business needs.

2) The requiring of periodic security assessments/penetration testing to evaluate the security posture of any business that stores or processes credit card transactions, to be performed by an independent information security consulting firm.

Finally, I want to offer what I have deemed to be the most important factor in security: the human factor. This is the essential, underlying all security issues, whether it's from deceptive credit card thieves or terrorist operatives that blend into our communities. This nation needs to train the community at large to recognize the deceptive tactics used by credit card and identity thieves to dupe into revealing their information, while still allowing individuals to retain the qualities of kindness and humanity that characterize the American people. I believe we as a people need not give up the qualities of trust and truth in order to gain strength against being duped and damaged. Training, training, training – and I believe it's essential to consider regulations that mandate security awareness training as part of an overall security program as required by HIPAA and GLBA. .

Now I will gladly answer any questions the members of the subcommittee would like to ask me.

***STATEMENT OF***

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION
WASHINGTON, D.C.

***BEFORE THE***

House Financial Services Subcommittees
on
Oversight and Investigations
and
Financial Institutions and Consumer Credit

***ON***

Fighting Fraud: Improving Information Security

April 3, 2003

1090 Vermont Ave., NW Suite 200, Washington, DC 20005 • T: 202-371-0910 • F: 202-371-0134 • www.cdiaonline.org

Chairwoman Kelly, Chairman Bachus, and members of the committees, thank you for this opportunity to appear at this joint hearing of your committees. For the record, I am Stuart Pratt, President and CEO of the Consumer Data Industry Association.

CDIA, as we are commonly known, is an international trade association representing approximately 500 consumer information companies that provide credit and mortgage reporting services, fraud prevention and risk management technologies, tenant and employment screening services, check fraud prevention and verification products, and collection services, as well.

We commend you for holding this hearing on the implications of breaches in information security at TCI Communications, DPI Merchants Services and TRIWest Healthcare Alliance. Specifically, your committees have asked us to comment on each of these breaches of security from the perspective of our members who operate as nationwide consumer credit reporting agencies.[1] In each case where we can comment, we have provided some background on the incident for purposes of context.

**TCI Communications:**

Background: On November 25, 2002, federal authorities announced they had arrested a man, 33-year-old Phillip Cummings, who had stolen passwords and codes, which gave him access to credit reporting systems. Cummings was a help-desk employee at Teledata Communications, Inc. (TCI), a Long Island, N.Y.-based company providing lenders with software, terminals and

support related to accessing consumer reports for permissible purposes under the FCRA. Cummings appeared in the U.S. District Court in Manhattan on charges that he and another man downloaded the personal information of 30,000 individuals over a period of time and accessed reports from consumer reporting agencies using access codes assigned to several lenders including Ford Motor Credit, Co.

Nationwide Consumer Credit Reporting Agencies: Our members have no direct relationship, contractual or otherwise, with TCI, since it provides its services directly to lenders. Our members learned of the possibility that access codes for their systems had been compromised via contact with their customer, Ford Motor Credit and also through subsequent law enforcement contacts. Those of our members with a compromised access code recognized the potential seriousness of the situation and worked collaboratively with Ford Motor Credit, law enforcement and with affected consumers as the investigation unfolded.

Upon learning of the problem our members quickly assessed what steps were necessary to mitigate the possible risks for consumers whose files may have been accessed for fraudulent purposes. In polling our members with regard to the types of actions taken on behalf of consumers we identified the following steps were commonly taken:

- The consumers' files were, in some cases, temporarily blocked to prevent additional use pending a notification being sent. Note that proactively blocking access to a file is very draconian and would, for example, stop a consumer who was in the middle of a home mortgage approval process from successfully purchasing a new home.

[1] CDIA's members include all of the nationwide consumer credit reporting agencies: Equifax, Experian and TransUnion.

- Notification letters were sent to consumers, in some cases by Ford and in some cases by CDIA members, notifying them of the incident. Dedicated toll-free numbers were brought online by our members and these were included in the notifications sent to affected consumers and they were shared with Ford.
- Once consumers contacted CDIA members, they were offered a range of services not require by law: 1. free file disclosures; 2. they were opted out of prescreened offers of credit; 3 a fraud alert was added to the file; 4. free access to additional file disclosures during the next 90 days following contact; 5. they were also offered free access to file monitoring services which can notify a consumer of changes in addresses, the inclusion of new accounts or negative information in their files, and also notification of who is accessing their files.

Beyond the priority of assisting consumers whose files may have been compromised, our members also took proactive steps to ensure that the scope of the fraud was contained. They conducted analyses of other passwords and sub-codes related to customers of TCI and other similar third-party vendors. They deployed pattern-recognition tools and initiated reviews to ensure that they could identify other anomalies related to access code usage.

The degree of law enforcement contact varied depending on the CDIA member. Our members did, however, cooperate with law enforcement in setting up sting operations and conducting other internal audits, which helped in these investigations.

**DPI Merchant Services:**

Our members reported to us that to date they have not been contacted with regard to this incident and therefore we do not have any information to add to the record.

**TriWest Healthcare Alliance:**

Background: The situation with TriWest was very different from that of TCI. News accounts report that individuals were able to steal hard drives from TriWest's data center. These hard drives contained information on approximately 500,000 military families.

Nationwide Consumer Credit Reporting Agencies: Since TriWest is not a customer of any of our members, there was understandably less immediate coordination. TriWest, as we understand it, did take quick action to notify all of the families and apparently this notice did recommend that affected families should take a number of steps to mitigate risks, including contacting nationwide consumer credit reporting agencies.

Many families followed the instructions in the TriWest letter and did contact our members. Consumers who contacted our members indicated that they were concerned that they were victims of fraud and thus they received free file disclosures.[2] TriWest did remain proactive beyond the letter they sent and contacted CDIA's members to request their coordination of some additional steps for the affected families and our members did voluntarily work with TriWest to

[2] Since CDIA's announcement in March of 2000, our members have executed a three-step process for any consumer who indicates that he/she is a victim of identity theft. These steps include the automatic inclusion of a fraud alert in the file, opting the file out of any non-initiated offers of credit and ensuring that the file disclosure is in the mail within three-business days. Included at the end of this testimony is a complete summary of all of the CDIA's efforts to assist victims.

**Summary:**

As we can see by the three examples above, security breaches can occur in a variety of ways including hacking, but also through the common criminal behavior of an employee. We believe there are some important points to consider stemming from our members' experiences with these incidents and with others that were not the subject of this hearing.

- Where the criminal behavior of an employee involves accessing information from a consumer reporting agency, through the illegitimate use of legitimate access codes or otherwise, the Fair Credit Reporting Act (15 U.S.C. Sec. 1681q) stipulates that this is an offense which can result in fines and imprisonment under Title 18 of the U.S. Code. These actions are also a violation of the "Counterfeit Access Device and Computer Fraud and Abuse Act of 1984" (18 U.S. C. Sec. 1030).[3] We applaud the fact that law enforcement aggressively investigated the TCI case and caught the perpetrator. Increased resources are necessary for law enforcement to continue to build on this effort and we should evaluate the value of increasing the penalties relative to these crimes.
- We must begin to learn to measure the risks relative to various breaches of information. Not all security breaches necessarily result in large-scale identity theft. In 2002, the state of California reported that they believed that more than 200,000 names of state employees had been stolen. Like the TriWest situation, state employees were instructed, unbeknownst to our members, to contact them. Our members voluntarily cooperated with the state in coordinating efforts, and one of our members reports that not a single

within three-business days. Included at the end of this testimony is a complete summary of all of the CDIA's efforts to assist victims.

[3] This amendment was enacted via PL 98-473 – October 12, 1984

dispute has been submitted relative to any of the file disclosures sent to CA state employees.

- Our members voluntary efforts to assist other companies which have experienced a security breach is taking a toll on our members' ability to service other consumers, including other victims of identity theft. One member reports that the costs of servicing the families of TriWest reached $1.5 million. We are not questioning the necessity of ensuring that military families received every level of support necessary during this time in our nation's history. But in the long run, our members cannot be placed in the ongoing position of having to bear a significant financial burden for every breach of information where the cause of the breach was not related to our members' data security practices[4] and where it did not involve our members' data.
- Coordinating assistance for consumers is important and as you can see in the attached summary of our efforts to assist verified victims of identity theft, we have taken and will continue to take action to ensure that victims of crimes are effectively served.

We appreciate this opportunity to testify and share our views.

---

[3] This amendment was enacted via PL 98-473 – October 12, 1984

[4] Note that the CDIA's members which operate as nationwide consumer credit reporting agencies are now governed by new security protocols which are established via the enactment of the Gramm-Leach-Bliley Act and the subsequent GLB Safeguards Rules. Included with this testimony is a summary of those rules.

## GLB Rules on Information Safeguards

**Source of Authority:** The GLB Act required the federal agencies responsible for financial institutions to adopt appropriate standards for financial institutions relating to safeguarding customer records and information. All financial institutions now operate under these rules.

**Purpose of Safeguards Rules:** To establish appropriate standards for financial institutions to relating to administrative, technical, and physical safeguards for customer information.

**Specific Objectives:** The objectives of these safeguards are:

- To ensure the security and confidentiality of customer information and records;
- To protect against any anticipated threats or hazards to the security or integrity of customer records; and
- To protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

**What the Rules Require:** The agencies' rules and guidelines contain consistent requirements. Each financial institution must:

- Develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards;
- Designate an employee (or employees) to coordinate its information security program;
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alternation, destruction, or other compromise of information;
- Assess the sufficiency of any safeguards in place to control these risks;
- Assure that contractors or service providers are capable of maintaining appropriate safeguards for the customer information, and require them, by contract, to implement and maintain such safeguards; and
- Adjust the information security program in light of developments that may materially affect the financial institution's safeguards.

## NEW BANK EXAMINATION PROCEDURES FOR INFORMATION SECURITY

On January 29, 2003, the FFIEC announced it is issuing revised guidance for bank examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of control and applicable management practices of financial institutions.

The new guidance supplements the "Safeguards" guidelines adopted by the FFIEC member agencies to implement the GLB requirements for standards to safeguard customer information. The new guidance is contained in the Information Security Booklet, a comprehensive105-page update to the *1996 FFIEC Information Systems Examination Handbook.* The Information Security Booklet describes how a financial institution must protect and secure the systems and facilities that process and maintain information. It requires both financial institutions and their technology service providers to maintain effective security programs, tailored to the complexity of their operations.

The Information Security Booklet replaces existing guidance on information security. It incorporates significant changes in technology since 1996 and incorporates a risk-based examination approach. Bank examiners will use these new standards in:

- Determining the level of security risks to the financial institution; and
- Evaluating the adequacy of the financial institution's risk management.

The federal agencies that comprise the FFEIC – the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision – have distributed electronic copies of these booklets to financial institutions and their technology service providers.

***Consumer Reporting Agency Responses to Identity Fraud***

- 1993. CDIA, then known as ACB, formed a Fraud and Security Task Force.

- 1998. Creation of True Name Fraud Task Force led by former Vermont Attorney General M. Jerome Diamond. The work of the task force included meetings with law enforcement, consumer organizations, privacy advocates, legislators and staff, victims, and others.

- The capstone of the True Name Fraud Task Force was a series of initiatives announced in March 2000. These initiatives meant the consumer reporting industry was the first industry to step forward and not merely educate its members about the problems consumers experienced, but to seek specific changes in business practices. The initiatives are:

    - Advocate the use and improve the effectiveness of security alerts through the use of codes transmitted to creditors. These alerts and codes can help creditors avoid opening additional fraudulent accounts.
    - Implement victim-assistance best practices to provide a more uniform experience for victims when working with personnel from multiple fraud units.
    - Assist identity theft victims by sending a notice to creditors and other report users when the victim does not recognize a recent inquiry on the victim's file.
    - Execute a three-step uniform response for victims who call automated telephone systems: automatically adding security alerts to files, opting the victim out of prescreened credit offers, and sending a copy of his or her file within three business days.
    - Launch new software systems that will monitor the victim's corrected file for three months, notify the consumer of any activity, and provide fraud unit contact information.
    - Fund, through ACB, the development of a series of consumer education initiatives through ACB to help consumers understand how to prevent identity theft and also what steps to take if they are victims.

- 2001. CDIA announced a police report initiative so that when a police report is provided as part of the process of disputing fraudulent data, Equifax, Experian and TransUnion will block these disputed items from appearing on subsequent consumer reports regarding that individual.

    - "Another collaborative effort with tremendous promise is your new police report initiative...I appreciate that certain consumer-based initiatives require you to balance accuracy issues - knowing that the consumer's report contains all relevant credit information, including derogatory reports - against customer service. From my

perspective, your police report initiative strikes just the right balance." *J. Howard Beales, III, Director of the FTC's Bureau of Consumer Protection, before the Consumer Data Industry Association. Jan. 17, 2002.*

- 2002. ID Fraud Victim Data Exchange. CDIA and its members committed to start a pilot test so that when an ID fraud victim calls any one of the participating credit reporting agencies, the victim will be notified that his or her identifying information will be shared by the receiving credit reporting agency with the other two participating credit reporting agencies and that the following steps will be taken by each recipient of the victim's information:
    - A temporary security alert will be added to the victim's file. This security alert will be transmitted to all subsequent users (e.g., creditors) which request a copy of the file for a permissible purpose under the Fair Credit Reporting Act.
    - The victim will be opted out of all non-initiated offers of credit or insurance.
    - The CRA will ensure that a copy of the victim's file is in the mail within three business days of the victim's request.
- Our efforts are paying off.
    - *Most calls are prevention related.* CDIA members report a majority of consumers who contact fraud units are taking preventative steps and are not reporting a crime.
    - *Victims are learning of the fraud earlier.* According to an FTC report in June 2001, 42% of victims learn about the crime within 30 days or less, a full 10% less than in the prior report. CDIA estimates another 35% learn of the crime within one to six months and 7% learn of the crime in six months to a year.
    - *Victimization of the elderly is dropping.* In 2001, the FTC estimated that 6.3% of identity fraud victims were over 65, a .5% decrease from 2000.

## About CDIA

Founded in 1906, the Consumer Data Industry Association (CDIA), formerly known as Associated Credit Bureaus, is the international trade association that represents more than 400 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services.

For more information about CDIA, its members, or identity fraud or other issues, please visit us at www.cdiaonline.org or contact us at 202-371-0910.

December 2002

**Statement of Mr. Bob Weaver**

**Deputy Special Agent in Charge**
**New York Field Office**
**United States Secret Service**

**Before**

**The House Financial Services Committee**
**Subcommittee on Financial Institutions and Consumer Credit**
**and the Subcommittee on Oversight and Investigations**

**U.S. House of Representatives**

**April 3, 2003**

Chairman Bachus, Chairwoman Kelly, Congressman Sanders, Congressman Gutierrez and members of both subcommittees, I appreciate the opportunity to participate in this important hearing.

I look forward to discussing with you today the successes of the Secret Service's New York Electronic Crimes Task Force (NYECTF), and the contributions we have made to the prevention of technology-based crimes, and the protection of our financial and critical infrastructures. I believe we have made a real difference in the effort to strengthen our economic security.

Task forces, in general, are not a new concept to law enforcement, and have been with us for some time. What makes the NYECTF so unique is the diversity of our membership and the personal, trusted relationships that develop between our members. Today, the task force consists of over 250 individual members representing federal, state and local law enforcement, the private sector, and academia. Our members include the largest financial services, telecommunications, and technology companies in the country. It also includes computer science specialists from 18 different universities. Among these partners, most of whom are strong competitors in the consumer marketplace, there is an unprecedented sharing of expertise, information and proven solutions, all of which have been employed in our common mission to prevent the disabling or compromise of critical systems and infrastructure.

Since 1995, the New York task force has charged over 1,000 individuals with electronic crime losses exceeding $1.0 billion. It has trained over 60,000 law enforcement personnel, prosecutors, and private industry representatives in the criminal abuses of technology and how to prevent them. The task force has identified tools and methodologies that can be employed by our partners to eliminate potential threats to their

information systems. We consider the NYECTF to be the 21st century law enforcement model that modernizes criminal justice and incorporates partnerships and information sharing within its core competencies. The NYECTF applies a systematic approach of protection, preparedness, detection and prevention directed at electronic crime.

This approach has been implemented successfully in various venues around the country. Pursuant to the Public Law 107-56, the USA/PATRIOT Act of 2001, the Secret Service has established Electronic Crimes Task Forces (ECTFs), based on our New York model, in Boston, Miami, Charlotte, Chicago, Las Vegas, San Francisco, Los Angeles, and Washington, D.C. These task forces are applying the blueprint and the methodologies of the NYECTF to develop partnerships and programs that are best suited to the needs of their individual communities. We never lose sight that one of the central tenets of the Secret Service's historic investigative mission is to serve the communities we protect.

The systemic approach of the task force is based on a business model. Its methodology incorporates the principles of preparedness, prevention, detection, response, education, training and awareness, pre-incident response risk management, investigations, and prosecution. This holistic approach combines a business strategy with a cultural change, producing a unique "teamwork" concept targeting risk management, crisis management, disaster recovery, best practices, due diligence, pre-incident response planning, and enterprise protection planning.

The NYECTF is a government success story, highlighted by an unparalleled sharing of information, a unique ability to analyze data with a diversity of partners, and a community-centered civil defense focus for the protection of our national security.

I believe what separates and distinguishes this task force from all others is our commitment to building trusted partnerships and placing the highest priority on that which is in the best interests of the community. Our commitment and contribution to the community is the greatest strength of the New York task force. Our core mission has always been simple -- to make a difference, to have an impact on the community, and to respond to the needs of our law enforcement partners, consumers, and private industry. The community has always been and always will be our focus.

On September 11, 2001, the Secret Service lost its New York Field Office in the collapse of 7 World Trade Center. Our office was destroyed and most of our criminal records, equipment and even personal effects were lost. But it was the community that we serve that stepped in almost immediately to help us rebuild.

I cannot tell you how proud I am of not only the men and women of the Secret Service who work tirelessly on the task force day and night but also the assistance and support of our task force partners – support that can never be quantified. As a result of their support, the New York task force became operational within 48 hours of the terrorist attack and immediately began fighting back.

The most compelling testimony to the expertise and success of the NYECTF is the large number of regular requests received from local and foreign law enforcement agencies for either training or consultation in support of their own initiatives and programs.

These requests have come from agencies nationwide, as well as foreign countries such as Australia, Bulgaria, Canada, England, Ireland, India, Italy, Japan, the Philippines, and Thailand. The Secret Service recognizes the need to promote international cooperation and remains proactive in the dissemination of information to law enforcement agencies, both domestically and internationally, regarding program initiatives and current telecommunications, financial and electronic crime trends. We are committed to working closely with our foreign law enforcement counterparts in response to cyber crime threats to commerce and financial payment systems. We currently have 18 overseas field offices and a permanent assignment at Interpol, as well as several other international initiatives. Our foreign presence increases our ability to become involved in foreign investigations that are of significant strategic interest to the United States.

As a footnote, the New York task force meets regularly with representatives from Wall Street, The Clearing House, Financial Services Round Table, Security Industry Association, Financial Services Sector Coordinating Council, Treasury Department, and the Financial Services Information Sharing and Analysis Center (FS/ISAC). The role of the FS/ISAC is to facilitate the sharing of information related to cyber threats and vulnerabilities within the financial services industry. The Secret Service is exploring common areas of interest with the FS/ISAC, including information sharing and information technology, as well as expertise in technical and physical security.

Over the last two decades, the U.S. financial services industry has benefited greatly by advances in e-commerce and telecommunications. The same technological developments that have so significantly contributed to the financial services industry's growth and importance, however, have also provided increased opportunities for electronic crime. Our task force recently hosted the New York Financial Services Industry Interactive Exercises for Critical Infrastructure Preparedness. These exercises are commonly referred to as "table top" exercises and are designed to address critical infrastructure security issues facing financial institutions. They facilitate interaction and communication on these issues among senior financial executives, financial industry trade associations, subject matter experts, academia and government officials.

These exercises will build upon the development of a new trusted relationship between the government and the private sector. Just like our task force, the table top exercises will foster personal interactions, networking opportunities, and give all who participate valuable information as well as avenues for resolution to future potential problems.

In today's high tech criminal environment, the challenge to federal law enforcement and government is to identify existing repositories of expertise and provide a framework for inclusion and productive collaboration among the many government agencies and their respective industry and academic counterparts. The Secret Service is convinced that

building trusted partnerships with the private sector and local law enforcement is the model for combating electronic crimes in the Information Age.

That concludes my prepared statement, and I would be happy to answer any questions that any of the members of the two subcommittees may have.

Dr. William Winkenwerder, JR., MD
ASSISTANT SECRETARY OF DEFENSE (HEALTH AFFAIRS)
HEARING ON INFORMATION SECURITY

***Introduction***

Mr. Chairman, Distinguished Committee Members, I want to thank you for the opportunity to address you, and to report on the Military Health System (MHS) Information Security and the TriWest Computer Information Theft. The protection of beneficiary health care information is of the utmost importance to the MHS. Extreme care and diligence have been taken to put in place the appropriate safeguards to protect this information.

***TriWest Computer Information Theft Overview***

On Saturday, December 14, 2002, there was a physical break-in of the TriWest Healthcare Alliance Corporate II offices in Phoenix, Arizona. Computer equipment and petty cash were stolen. On Monday, December 16, 2002, the theft was discovered, police and investigative authorities were contacted and the TRICARE Management Activity (TMA) Operations staff was notified. On Tuesday, December 17, 2002, back up tapes were run to restore computer operations (30 hour process). Health Affairs/TMA was notified of beneficiary information theft on Friday, December 20, 2002. The information that was stolen included: beneficiary names, addresses, phone numbers, social security numbers, some claims information with relevant procedure codes, and personal credit card information on 23 individuals. To date, TMA has not received notification of any verified cases of identity theft related to TriWest stolen computer equipment.

***Actions Taken in Response to the TriWest Theft***

Several steps have been taken to communicate with all affected beneficiaries. During December 21-31, 2002, TriWest mailed 562,797 letters to affected beneficiaries notifying them of the theft and providing information on how to protect against identity theft. TriWest mailed a second letter in early February 2003, with additional information to assist beneficiaries with reporting fraud online to Credit Reporting Agencies and provided the appropriate form for verifying if their SSNs were included on stolen computer equipment. An around-the-clock communication link with beneficiaries was established via Web, toll-free telephone numbers and e-mail. More than 66,000 web queries, 37,500 calls and 10,300 emails have been received. The 23 individuals who may also have had personal credit card information compromised were contacted by phone and informed of the incident and proper actions to be taken in response. I met with beneficiary groups and described the corrective actions being taken.

A number of additional actions were conducted in response to this theft. A government team was dispatched to TriWest, December 22-24, 2002, to make an initial impact assessment. I conducted daily conferences with leaders from the MHS, Defense Criminal Investigative Service (DCIS), and TriWest. Information about the potentially compromised data was provided to the Social Security Administration and Federal Trade Commission. A $100,000 reward for information leading to conviction of individuals responsible was posted by TriWest. A review of security language in current and new TRICARE contracts was initiated to ensure incorporation of strong security requirements.

I requested that all TRICARE contractors perform a physical security assessment of their facilities using a government developed matrix composed of the Defense Information System Agency (DISA) Physical Security checklist and industry best practices. The majority of the physical security assessment results were received by January 1st and the remaining assessments were submitted by January 21st, 2003. On-site validation of the contractors' assessments were conducted by government teams and completed by February 7, 2003. The TRICARE contractors have provided timelines to address the mitigation of deficiencies identified during the assessment process. These actions have further strengthened the TRICARE contractors' overall security posture in terms of protecting our beneficiaries health care data. I requested that the Service Surgeons General also conduct a physical security assessment of all their military treatment facilities using the same matrix. The Services' assessment has been completed and each Service is developing measures and timelines to correct deficiencies.

Additionally, I asked that the Department of Defense (DoD) Inspector General's (IG) office conduct a rapid assessment of the physical information safeguards in place at a sampling of TRICARE contractor sites and DoD medical treatment facilities (MTFs) where patient-sensitive electronic data are stored. The IG is currently conducting assessments at a number of MTFs and TRICARE contractor sites. The report will be available in September 2003.

I formed a Health Information Security Working Group (HISG) comprised of senior representatives for HA/TMA, Service Surgeons General, Command, Control, Communications and Intelligence, Defense Management Data Center, DISA, and TRICARE Contractors. This work group, with support from information systems experts, is currently reviewing security practices and will make recommendations, as needed, for additional requirements for information security. The first meeting occurred on January 14, 2003 to examine commercial and DoD information security best practices, review regulatory requirements and discuss physical security self assessment check lists. On March 28th 2003, TMA

conducted a follow up meeting through the HISG, to review and discuss the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Information Technology Personnel Background Investigation requirements, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulatory requirements, and the DISA Physical Security and industry best practice matrix.

It should be noted that in 1967, a decision was made to use the SSN as the universal identifier for the Department of Defense (DoD). The decision was made to avoid the use of separate personal identifiers within the Medical, Financial, and Personnel communities of DoD. Additionally, the SSN is the one number that connects DoD to other Federal Agencies such as Department of Health and Human Services and the Social Security Administration. To move to a separate identifier would negatively impact the services provided to TRICARE beneficiaries.

***Military Health System Information Security***

The Military Health System (MHS) Information Security (IS) Program vigilantly protects patient information of Service members, military retirees, and beneficiaries in accordance with Federal and Department of Defense (DoD) policies and guidance. The MHS IS Program does this by enhancing the integrity, availability, confidentiality, non-repudiation, and authentication of MHS Automated Information Systems (AISs) and networks that support military medical readiness and peacetime health care.

This program monitors IS operations to ensure critical health care information is available throughout DoD's Global Information Grid. It also ensures critical health care information is managed consistently with defense in depth methodology and evolving DoD IS Strategic Goals of protecting information, defending systems and networks, providing IS situational awareness and IS command and control, improving and integrating IS transformation processes, and creating an IS empowered workforce.

The MHS IS Program accomplishes its missions by utilizing a variety of government and industry security assessment resources and tools to continuously strengthen the MHS security program and plans. The program performs comprehensive risk assessments which test security controls. Third party assessments of MHS Security Program are frequently conducted to validate that policies and practices align with government and industry best practices such as the Information Assurance Vulnerability Management program, security practices

from National Institute of Standards and Technology, Computer Security Institute, Carnegie Mellon, General Accounting Office, Defense Information Systems Agency, etc.

This program maintains an IS empowered workforce through an aggressive training program which includes initial user security training and yearly refresher training via an automated Web-based IS security and awareness module for all users. Advanced training is also available through IS training media, including those provided by DISA, either through Web-based training and/or CD ROMs for individuals with significant security responsibilities. Formal classroom training and professional seminars are coordinated to promote and expand IS knowledge (e.g., coursework from The National Defense University such as Information Security Common Body of Knowledge; Critical Information Systems Technologies; Managing Information Security in a Network Environment; and Assuring the Information Infrastructure.)

The MHS information security program aligns with DoD security regulations and guidelines to include the DoD Information Technology Security Certification and Accreditation Process and DoD Information Technology Personnel Background Investigation requirements. The MHS also provides strong representation on DoD IS workgroups. These DoD workgroups provide the direction for emerging DoD security requirements and assist in the preparation of DoD security requirements. The MHS IS workgroup, comprised of TMA, Army, Navy, Air Force, Defense Information Systems Agency and Joint Staff representatives, develops a single Tri-Service strategy for incorporating DoD information security requirements into the MHS. Coordination through the MHS IS workgroup has resulted in a cohesive medical process for addressing dynamic DoD information security requirements.

The MHS has been a leading partner in the development of health information security and privacy standards at the national level. Under the Health Insurance Portability and Accountability Act (HIPAA), representatives from the MHS have participated with federal agencies to include the Department of Health and Human Services, Department of Veterans Affairs, Food and Drug Administration, Centers for Disease Control, Social Security Administration, and Centers for Medicare and Medicaid Services, in crafting the regulations that define health information privacy and security protections. Over the last two years, the MHS has diligently worked to meet the HIPAA Privacy regulation by the April 14, 2003, implementation date. With the recent publication of the HIPAA security rule on February 20, 2003, and the directed implementation deadline of April 15,

2005, the MHS will execute a comprehensive analysis of the regulation and finalize a plan for implementing HIPAA security throughout the MHS.

***Conclusion***

Mr. Chairman, we take seriously our responsibility to protect the privacy and confidentiality of the patient information for our Service members and our broader military family.

Extensive efforts to further enhance physical security are ongoing. Based on outcomes of ongoing assessments, DoD will determine if additional resources and support are required to plan, program and implement new requirements.

Thank you for the opportunity to testify before your Committee on this important issue.

**U.S. Department of Justice**

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 30, 2003

Mr. Hugh Nathanial Halpern
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Halpern:

In your letter dated April 18, 2003, you enclosed two questions from Congresswoman Sue Kelly. For the hearing record, the following responses are provided:

**Question 1:** Do you have a special task force to monitor foreign attempts at data intrusions? Do you share that information with other government agencies?

**Answer:** The FBI's Cyber Division manages a national program for investigating counterterrorism and counterintelligence computer intrusions. There is a Unit at FBI Headquarters dedicated to these matters, and all FBI field divisions have personnel assigned to these investigations. We work closely with the Intelligence Community and the Inspectors General, sharing information while focusing on particular foreign threats, and coordinating and de-conflicting investigative efforts.

**Question 2:** Does the FBI have the necessary funds and/or manpower to investigate crimes related to security breaches?

**Answer:** The Cyber Division is working closely with the House and Senate Appropriation Committees, along with the Department of Justice, to ensure that the transfer of Cyber Division assets to the Department of Homeland Security does not impact on our ability to address computer intrusions. The FBI has launched an extensive recruiting effort to ensure that we have properly trained investigators working on cyber cases.

Sincerely,

Jana D. Monroe
Assistant Director
Cyber Division

**Response of Evan Hendricks, Editor/Publisher, *Privacy Times*, to questions from Subcommittee Chairwoman Sue Kelly.**

Question 1: "You speak of people having access to 'their own' data. Do individuals have a property interest in 'their' data?

Under U.S. v. Miller and other rulings by the U.S. Supreme Court, individuals do not have a property interest in personal data held by third parties such as banks. This is why there is such a tremendous tension over this issue: many Americans think that information about themselves is "theirs" or should be theirs. For example, if you were speaking to a group of constituents and told them that information about them is not theirs, and that the law does not give them adequate control over it, I am confident you would receive some interesting responses.

In 1976, the U.S. Privacy Protection Study Commission, a bipartisan commission created by the U.S. Privacy Act of 1974 to study private sectors issues, said the U.S. v. Miller case underscored the need for Congress to enact statutory law, based upon "Fair Information Practices," so that privacy would be adequately protected. One reason that Gramm-Leach-Bliley will not be the "last word on privacy" is that it fails to live up to Fair Information Practices standards.

Question 2: "When an individual interacts with another entity, does the other entity have any interest (property or otherwise) in the data that is generated from that interaction?"

Yes. The problem, from a privacy point of view, is that the individual too often does not have a sufficient "legal interest" in his or her own data, in part because of the absence of adequate statutory law.

Question 3: "You have criticized the handling of the DPI case, including the apparent 'shroud of secrecy' around how the payment card companies the

matter. Can you tell me whether a single card number was actually taken from DPI?"

No. I could only answer that if I had legal authority to investigate the case, which of course I do not have. John Brady, MasterCard Vice President for Merchant Fraud Control, indicated in his prepared statement that nobody knows, stating: "Although it is not clear at this point how much data the hacker successfully exported from the DPI system, we do know the hacker potentially had access to approximately 10 or 11 million Visa, Discover, American Express, and MasterCard payment card account numbers and expiration dates."

Question 4: Can you tell me whether there has been one instance of fraud which resulted from the DPI incident?

No.

Question 5: Is it not something of a success story that all parties involved took immediate action and, to date, their efforts have paid off?

Hopefully, it will continue to be true that no fraud resulted from this hack. I also agree that it appears that many of the institutions involved responded quickly.

But I maintain that the inability of consumers to know that their credit card numbers were compromised represents a failure that public policy should cure, as the California law attempts. In my opinion, best practices dictate that there is a reasonable mechanism for notifying individuals so they can be on the lookout for misuse of their personal data. Clearly, law enforcement believes that crime prevention is enhanced by increasing the number of individuals who are active in detecting fraudulent activity.

**TriWest Healthcare Alliance**
**David J. McIntyre, Jr., President and CEO**
**Responses to Questions from Mrs. Kelly**
**April 3, 2003 Hearing**
**"Fighting Fraud: Improving Information Security"**

**Question 1.** **Was the consumer information on the stolen hard drives encrypted, and have you considered the use of encrypting account numbers and other sensitive identifying information to better protect against theft?**

Answer: As I mentioned during questioning by Congressman Moore, there is certain information related to the theft of the computer equipment and the patient record information contained within that I am unable to discuss at this time due to the ongoing investigation by the Defense Criminal Investigative Service (DCIS) and the Federal Bureau of Investigations (FBI). That said, we do use various types of encryption for different applications where data needs to be secured. This includes information on our website (www.triwest.com). Encryption alone, however, is not a guarantee that the information encrypted is totally secure, so TriWest has implemented other safeguards as well in order to protect beneficiary information.

**Question 2.** **It seems as though the crime at TriWest involved someone who must have known where the security cards were and where sensitive computer data was kept. Does TriWest do any background checks with respect to employees that have access to these tools or data?**

Answer: As mentioned during my oral testimony, the individual who physically broke in to TriWest's facilities did so using the "master" electronic key card located in the facility manager's office. While there has certainly been speculation as to whether or not this crime was tied to staff affiliated with TriWest or with the property management's operations, TriWest has no insight as to the investigational leads identified by DCIS or the FBI. TriWest has been totally forthcoming with information requested by these two investigative agencies on current and former TriWest employees, and we are aware that many of those individuals have been interviewed.

TriWest, as part of its hiring process, does reference checks on individuals who would have access to the type of computer equipment that was stolen. Additionally, as part of a DoD-wide accreditation process that was started (but not completed) prior to the theft, known as the Defense Information Technology Security Certification and Accreditation Process (DITSCAP), additional background checks (including fingerprinting) are currently required on any TriWest employees who will have electronic access to beneficiary data. All

TriWest employees are required to completed paperwork for the government personal security investigations. These documents (which included fingerprints for each individual) are forwarded to the US Office of Personnel Management (OPM) for processing.

**Question 3: Prior to the break in, did TriWest have a written data security program that was approved by you or other senior management?**

Answer: Prior to the break-in, TriWest did have written policies and procedures in place relative to the security and privacy of beneficiary information in all forms, to include information contained on TriWest computer equipment.

**Question 4. Your company is directly responsible for the loss of information involving hundreds of thousands of individuals. Yet your statement suggests that truncating credit card account numbers on receipts would protect consumers against identity theft. In light of your knowledge benefits of truncating account numbers, did your systems truncate individual's social security numbers or account numbers, either when used internally or when provided to your customers on bills, invoices, and the like? Should Congress require health insurance companies to truncate social security numbers and account numbers which are used internally or which are provided to customers on documents?**

Answer: As noted in my oral testimony, I have personally observed that my credit card information is sometimes listed on receipts and other statements with my full credit card number and the corresponding expiration date, while many companies are only using numbers which show the last four digits. Additionally, many organizations, including the Senate and House Credit Unions, still utilize full social security numbers when providing information on balance inquiries and other statements. While the current trend of identity theft would certainly lead one to believe that it is appropriate to truncate these types of identifiers, the business community and the federal government still follow the practice of full disclosure of these types of identification.

Currently, TRICARE policy requires that the military sponsor's full social security number (SSN) be placed on documents such as explanations of benefits, authorization letters and other documents. As a TRICARE government contractor, we must comply with these requirements. Please note that TriWest has elected to truncate SSNs in certain applications that are not required under our TRICARE contract (such as the SSN verification form we added to our website for individuals to determine if their individual SSNs were included on the stolen computer equipment).

TW supports truncating SSN's as a cost-effective alternative to protect this means of identifying beneficiaries. Any effort to move to a different identifying system would be prohibitively expensive.

**Question 5: What federal requirements apply to TriWest with respect to information security? If there are any, do you believe that TriWest was in compliance? If there are not any, why shouldn't Congress address this issue?**

Answer: At the time of the break-in, our TRICARE contract and the TRICARE Operations Manual both contained certain security requirements. TriWest was in compliance with those requirements. As mentioned in Question number three, DITSCAP (DoDD 5200.40) is a new requirement for DoD contractors. The primary purpose of DITSCAP is to protect and secure the information systems and other elements that make up the Defense Information infrastructure. DITSCAP applies to any DoD system that collects, stores, transmits or processes unclassified, sensitive or classified information. Security Information Management is the emphasis of the DITSCAP security audit and certification process. It is a continuous approach that includes:

- System identification
- Threat definition
- Vulnerability determination
- Risk Analysis
- Countermeasure Recommendation
- Residual Risk Assessment

TriWest was granted Interim Approval to Operate under DITSCAP on March 28, 2003. Together, with all the other TRICARE Managed Care Support Contractors, TriWest is working toward full accreditation.

Questions Submitted by Congresswoman Sue Kelly for Mr. Mitnick

**Are hackers deterred at all by our current enforcement mechanisms?**

Individuals that possess hacking skills may not necessarily use those skills in a socially unacceptable way. For those that do, it is difficult to class "hackers" into a single group because of the varying motivations or desired objectives. Most people that commit criminal acts are not deterred because of current enforcement mechanisms, but rather, assess their risk based on the potential of being identified and caught. I strongly believe the government should focus the deterrent in heightening the high risk of being detected and identified, rather than the consequences after the damage has been done. For instance, sophisticated hackers may hijack public wireless networks to accomplish their illegal acts to avoid detection, but if camera surveillance could document their presence near the wireless access point, it may deter illegal activity.

**What should be the minimum standard for an information security audit that regulators should expect from financial institutions? And are there any best practices guidelines that can be widely applicable?**

A meaningful and effective security audit should be comprised of an established baseline for that vertical. It may not be cost effective in attempting to identify each and every security weakness, but rather, to concentrate on managing the security risks that could result in significant losses to the enterprise.

The minimum standard for an information security audit should not focus on Internet-based vulnerabilities. The attacker's objective is to exploit any vulnerability in the entire "system" to accomplish his or her objective. Therefore, an effective security audit must also examine the controls in physical, administrative, technical, and personnel security for potential weaknesses that could be exploited by a resourceful adversary.

After performing a risk assessment, regulators should also examine the information flow of valuable information assets to identify the specific access points which can be used to compromise the confidentiality, integrity, and availability of such information. The auditors must not overlook the potential vulnerability of the human element, whereby the attacker uses manipulation and deception ("social engineering)" to influence a trusted insider into giving the attacker the keys to the kingdom. I firmly believe that financial institutions should undergo periodic penetration testing to identify potential weaknesses associated with technology and the people that work for the entity.

**You recommend requiring a two-factor form of authentication, including phone call verification for certain on-line purchases for verification. Could this second step be done more cheaply by having card retailers send automatic e-mail links to their websites for verification or notice?**

The above suggestion would be cheaper, but could easily be circumvented by credit card thieves.

The thief could just set up an e-mail account on a commercial or free service provider (Yahoo, Hotmail, etc.), under the credit card holder's name, and then use the newly created e-mail account when purchasing goods or services online. The merchant does not have the ability to verify whether the purchaser provided a legitimate e-mail address belonging to the credit card holder. One fraud mitigation technique may be to decline online transactions where the purchaser provides an email address using a free email service provider.

A thief could also set up a "legitimate" account under the card holder's name at a commercial provider (AOL, MSN, etc.) using stolen credit card details or a low-value prepaid credit card to effectively impersonate a credit card holder.

The credit card ***issuer*** may require their customers to file a valid e-mail address before authorizing card holder "not-present" transactions. To be effective, a verification process would have to be developed and implemented which would allow the merchant to verify the customer's provided e-mail address that is on-file with the credit card issuer prior to sending the hyperlink to verify identity, but this step would require some access to the card credit issuer's database, would require the card issuer to share this limited information with third parties, or require participation in the verification process by the credit card issuer.

An obvious weakness in this approach is the credit card thieves can determine the card credit issuer by examining the bank identification number (BIN) which can be determined by examining the first six digits of the card number. Once the issuing bank is identified, the thief can call the bank and based on knowing the card holder's non-public personal identifying information, can pretext the customer service representative into changing the customer's email address. In this instance, the issuer should send a notification to old e-mail address advising the purchaser of the change of e-mail address.

Additionally, this approach only authenticates the credit card holder based ***only*** the provided e-mail address, which may be verified or unverified by the card issuer. A possible solution would be to have the card issuer or a trusted third party, establish an outgoing connection to the purchaser **at the time of purchase**, requiring the customer to prove identity by entering a Personal Identification Number or some other shared secret. In this instance, the verification process is performed over a different, albeit, an online channel.

I understand that nCipher, (www.ncipher.com), a credible company that develops cryptographic security solutions, has developed, or is the process of developing a verification solution similar to the one described above.

I encourage the Committee to review such security products, and require financial institutions to develop and implement security processes that focus on authenticating the card holder's identity rather than attempting to regulate the secrecy of non-public personal identifying information. The latter will never work.

Thank you.

Kevin Mitnick
2219 E. Thousand Oaks Blvd. #432
Thousand Oaks, CA. 91362
(310) 689-7229