AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

IDENTITY THEFT PENALTY ENHANCEMENT ACT, AND THE IDENTITY THEFT INVESTIGATION AND PROSECUTION ACT OF 2003

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

ON

H.R. 1731 and H.R. 3693

MARCH 23, 2004

Serial No. 74

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

92–671 PDF WASHINGTON : 2004

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

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

TOM FEENEY, Florida
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
MARK GREEN, Wisconsin
RIC KELLER, Florida
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia

ROBERT C. SCOTT, Virginia
ADAM B. SCHIFF, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts

JAY APPERSON, *Chief Counsel*
ELIZABETH SOKUL, *Counsel*
KATY CROOKS, *Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MARCH 23, 2004

OPENING STATEMENT

	Page
The Honorable Howard Coble, a Representative in Congress From the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security	1
The Honorable Robert C. Scott, a Representative in Congress From the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security	2
The Honorable John Conyers, Jr., a Representative in Congress From the State of Michigan, and Ranking Member, Committee on the Judiciary	4
The Honorable Adam B. Schiff, a Representative in Congress From the State of California	4

WITNESSES

Mr. Timothy Coleman, Counsel to the Assistant Attorney General, Criminal Division, U.S. Department of Justice	
Oral Testimony	7
Prepared Statement	9
Mr. Larry D. Johnson, Special Agent in Charge, Criminal Investigative Division, United States Secret Service	
Oral Testimony	12
Prepared Statement	14
Mr. Robert F. Ryan, Senior Director, Government Relations, TransUnion	
Oral Testimony	17
Prepared Statement	20
Mr. Louis P. Cannon, President, District of Columbia Lodge #1, and Chairman, Federal Officers' Committee of the Grand Lodge, Fraternal Order of Police	
Oral Testimony	28

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared statement of Mr. Louis P. Cannon, President, District of Columbia Lodge #1, and Chairman, Federal Officers' Committee of the Grand Lodge, Fraternal Order of Police	41
Prepared statement of the Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas	43
Speech Given by United States Supreme Court Justice Anthony M. Kennedy at the American Bar Association annual meeting, August 9, 2003	49

IDENTITY THEFT PENALTY ENHANCEMENT ACT, AND THE IDENTITY THEFT INVESTIGATION AND PROSECUTION ACT OF 2003

TUESDAY, MARCH 23, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:05 a.m., in Room 2141, Rayburn House Office Building, Hon. Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good morning, ladies and gentlemen. The Subcommittee will come to order.

Mr. Bobby Scott, the distinguished gentleman from Virginia and the Ranking Member of the Subcommittee is en route. But since everyone is in place, I think we will go ahead and start even though it is a little after the starting time.

The Subcomittee on Crime, Terrorism, and Homeland Security will hold its first hearing on H.R. 1731, the "Identity Theft Penalty Enhancement Act," and H.R. 3693, the "Identify Theft Investigation and Prosecution Act of 2003."

This hearing examines the growing problem of identity theft in this country and what additional steps Congress, law enforcement, businesses and individuals can do to address the problem.

There has been a great deal of focus on this issue in Congress in recent years. H.R. 1731 and H.R. 3693 propose some additional steps Congress can take to minimize the threat of identity theft to the individual American companies and the security of our country.

H.R. 1731 would establish penalties for aggravated identity theft when the theft is related to or in furtherance of certain other criminal acts.

H.R. 3693 would provide $100 billion to the Department of Justice to investigate and prosecute identity theft crimes.

This hearing will examine the need for these bills as well as additional legislative proposals Congress should consider to address the growing problem of identity theft.

Identity theft and identity fraud are terms used to refer to all types of crimes in which an individual's personal or financial data is misused typically for economic gain or to facilitate another criminal activity. Identity crime is not directed at any one demographic. It affects all types of individuals regardless of age, gender, nationality or race.

In 1998, Congress enacted the Identity Theft and Assumption Deterrence Act directing the Federal Trade Commission to establish the Federal Government's central repository for identity theft complaints and to provide victim assistance and consumer education.

In 2002, the FTC received 161,819 victim complaints of compromised personal information. The FTC's statistics for 2003 determined that a total of 4.6 percent of survey participants indicated they were victims of some type of identity crime in the past year.

Identity crimes include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud and passport visa fraud. Identity crimes can be associated with a variety of other crimes such as mail theft and fraud, money laundering, immigration fraud, narcotics and weapons trafficking, and terrorism.

According to the FTC, theft, including lost or stolen wallets or the theft of a victim's mail was the most commonly mentioned way of obtaining the victim's personal information. Approximately 25 percent of identity theft victims reported that their information was obtained through such theft. Approximately 50 percent of the identity theft victims said they did not know how the person who misused their personal information obtained it.

These victims who did know the person who obtained their information, the FTC found that 23 percent indicated that the person responsible was someone who worked at a company or financial institution that had access to the victim's personal information. According to 13 percent of the victims, their information was compromised during a store purchase or purchases by mail, internet or telephone. Approximately 4 percent of the victims cited stolen mail as the point of compromise, and 14 percent of all victims claim their information was compromised by other means including family members and workplace associates.

Since September 11, 2001, the Federal and State officials have taken notice of this crime because of the potential threat to security, but the cost to the consumers and corporations is equally alarming. The FTC estimates the loss to businesses and financial institutions due to identity theft to be approximately $47.6 billion. The cost to individual customers are estimated to be approximately $5.5 billion. Additionally, victims have a difficult time consuming and expensive task of repairing a damaged credit record or history as well as their reputation.

As identify crime increases, we must find new ways to combat this compromise of personal information. Today, we will discuss additional steps that may be taken to address this continuing problem of identity theft. I want to thank the witnesses who were able to be here today and look forward to their testimony.

And now I am pleased to recognize the distinguished gentleman from Virginia, the Ranking Member, Mr. Bobby Scott.

Mr. SCOTT. Thank you Mr. Chairman. And I am pleased to join you in convening the hearing on H.R. 3693, the "Identity Theft Investigation and Prosecution Act of 2003," of which we are both cosponsors, and H.R. 1731, the "Identity Theft Penalty Enhancement Act," cosponsored by Representatives Carter and Schiff, a Member of this Subcommittee.

The two bills represent different approaches on the impact of the problem of identity theft. H.R. 3693 simply provides the money to dedicate resources to enforce existing law.

In its Identity Theft Survey Report issued last year, the Federal Trade Commission indicated that when asked what could be done to help fix problems that victims experienced as a result of identity theft, the action most frequently cited by the victims was to improve the investigation by law enforcement after the crime has been committed. Specific proposals mentioned include a stronger commitment to catching the thief or thieves, better follow-up and communication with the victim and increased assistance from law enforcement.

H.R. 1731 provides for mandatory penalties or enhancements for a host of identity-theft related crimes.

The FTC survey released last September showed that 27.3 million Americans had been victims of identity theft in the previous 5 years, including 9.9 million last year alone. According to the survey, last year's identity theft losses to businesses and financial institutions totaled nearly $48 billion while consumer victims reported about $5 billion in out-of-pocket losses and expenses.

The FTC survey reported only 26 percent of all victims contacted law enforcement agencies; only 17 percent of victims who suffered only the misuse of existing credit cards bothered to contact local law enforcement officers. That is why identity thieves operate with impunity using credit card or other stolen ID until it is cancelled and then moving on to the next victim.

Yet ironically, identity thieves are more susceptible to being caught than criminals in general because there is a significant paper trail left with their crimes. And that is what H.R. 3693 does—is developed to do. It provides the tools, the equipment, the training, manpower and needs to fill this gap and give more victims the confidence that they need to report the identity theft to law enforcement.

If properly investigated and prosecuted, there is an opportunity for a high rate of success on convictions. And once identity thieves are aware of the new order and the likelihood of prosecution instead of little likelihood of prosecution, they are less likely, in my judgment, to steal, and the practice will greatly be curtailed.

Now the approach in H.R. 1731 is different. We have, unfortunately, in that bill the same problems with mandatory minimums that we have seen in other legislation. The bill continues the tendency of Congress to violate the sense of proportionality and rationality in sentencing, which the Sentencing Guideline System and Sentencing Commission was designed to deal with sentencing in a proportional and fair manner.

Now, it imposes mandatory minimum sentences on a whole host of identity related crimes, many of which have nothing to do with theft. For example, the bill provides it to be a crime to represent that you are a citizen if you are not. That is not necessarily identity theft, but I suppose that we should increase the maximum allowable sentence for that crime, because some cases might warrant a more harsh sentence.

We should have a sense of proportionality and allow the judges to make the determination in individual cases with the sentencing guidelines.

While penalty enhancement for identity theft is appropriate, it is not appropriate in the manner of the bill that underlying crime warranting a 1-year sentence gets the same penalty enhancement as a crime warranting a 20-year sentence.

The prospect of adding a 2-year mandatory minimum to an offender who is willing to risk a 15- to 20-year sentence is not likely to have much of a deterrent effect.

Again, I favor penalty enhancements, but I do believe the impartial judge with all the facts and circumstances of the case and the offender before him with the adversarial presentation of the facts and evidence in the case is a better measure for the appropriate sentence than the mandatory minimum in that bill.

So I look forward to the testimony of the witnesses on this important issue, and I look forward to working with you, Mr. Chairman, as we try to reduce the problem of identity theft.

Mr. COBLE. I thank the gentleman. And we have with us the Ranking Member of the full Committee, the gentleman from Michigan, and also the sponsor of the other bill, Mr. Schiff, the gentleman from California.

Mr. Conyers, would you like to give an opening statement?

Mr. CONYERS. If I could, thank you, Mr. Chairman, and strike the requisite number of words.

I just wanted to welcome our witnesses and particularly Officer Cannon from the Fraternal Order of Police. We have been working together in this Committee for many years.

Well, what do we have here? We have the classic case of California conservatives wanting to put not one mandatory sentence in but three. Can you beat that? Finally, the Congress acts and what do we do? We overreact.

We want 5-year mandatory, 2-year mandatory and no probation. We, as legislators, now become the judge and make sure we remove some more judicial discretion from the judge in one of the bills.

Now, you know, it is about time we get down to business on this thing. That is no way to run a ship. We have got to start off first with a Coble-Scott bill that recognizes the problem, but three mandatory sentences and a removal of judicial discretion all in one little bill is a little bit overarching.

So I am happy to join the Chairman; the gentleman from Virginia; the gentleman from Massachusetts, Mr. Frank; gentleman from Texas, Mr. Frost; the gentlelady from Illinois, Ms. Schakowsky; the gentlelady from California, Ms. Lee; the gentleman from Ohio, Mr. Kucinich, in what I hope will be the bill that comes out of the Committee or some reasonable compromise thereto.

And I thank the Chairman for allowing me this opportunity.

Mr. COBLE. Thank the distinguished gentleman from Michigan.

The distinguished gentleman from California, would you like to be heard before we hear from our witnesses, Mr. Schiff?

Mr. SCHIFF. Yes, Mr. Chairman. I want to thank you for holding the hearing today on the serious issue of identity theft, including

the hearing on H.R. 1731, the "Identity Theft Penalty Enhancement Act," legislation that I join Mr. Carter in introducing.

I want to thank Ranking Member Bobby Scott and Ranking Member John Conyers for their work to combat identity theft as well and for the additional legislation that is the subject of the hearing today.

Identity theft topped the list of consumer complaints filed with the FTC for the last 4 years in a row. In September 2003, the FTC released a comprehensive survey concluding that a staggering 27.3 million Americans have been victims of identity theft in the last 5 years, costing consumers and businesses an estimated $53 billion in 2002 alone.

Formal reports of identity theft filed with the FTC are also on the rise. Earlier this year, the FTC reported that almost 215,000 cases of identity theft were reported in 2003, a huge increase from the previous 2 years. In fact, the home States of several Members of the Subcommittee are at the top of the list of identity theft victims in 2003, with Texas ranking number four and Florida ranking number five.

My own home State of California ranks number three in the number of victims of identity theft per capita, with over 37,000 complaints reported by consumers costing over $40 million last year. Nationally, California cities crowd the top 10 list of metropolitan areas with the highest per capita rates of identity theft reported. The Los Angeles Long Beach metropolitan area that includes my district is particularly prone to such crimes ranking number two nationally with over 13,000 victims.

This problem is not new. In fact, I can recall, in the late 80's and early 90's when I was with the U.S. Attorney's Office, having many of these cases in our office and prosecuting one myself. And when we obtained the search warrant to search the briefcase belonging to the defendant, we found, in this one briefcase, applications for employment with a savings and loan in one State, W–2s from a Montgomery Ward in a second State and, most interesting, the complete faculty list of Brandeis University with the Social Security numbers of all of the faculty.

These rings of identity theft are often extensive, and this was several years ago. The problem has only grown to epidemic proportions since then. Identity theft wreaks havoc on the lives of millions of hard-working Americans now. A victim of identity theft usually spends a year-and-a-half working to restore his or her identity and good name.

Many of my constituents—and I know my colleagues as well—have urged Congress to act quickly and effectively to crack down on this growing problem.

All forms of identity theft are problematic, but the stealing of one's identity for the purpose of committing other serious crimes, including murder and terrorism, is especially egregious and demands even stronger action. For this reason, I have joined my colleague, Mr. Carter, in introducing the Identity Theft Penalty Enhancement Act, legislation that will make it easier for prosecutors to target those identity thieves who steal an identity for the purpose of committing other serious crimes.

The bill stiffens penalties to deter such offenses and strengthens the ability of law enforcement to go after identity thieves and prove their case. The legislation also makes changes to close a number of gaps identified in current Federal law.

Identical legislation was introduced by Senators Feinstein and Kyl, passing unanimously in the Senate in January of 2003. The bill is also supported by the Justice Department and the FTC.

With advances in technology and the Internet, identity theft has been transformed from a basic street crime involving a stolen wallet or stolen pin number into a sophisticated crime. Nationwide computer networks have given hackers the ability to access a large number of identities that can be quickly shared with large organized networks or criminals.

Homeland security concerns have certainly heightened the need to protect against identity theft given the potential ease with which a terrorist can assimilate to and move about in our society with stolen identity documents. One such example is the case of a Massachusetts health club worker who stole the identities of at least 21 members of the health club and provided their names and financial details to Abdel Ghani Meskini, an al-Qaeda operative who later pled guilty to conspiracy for his role in attempting to blow up the Los Angeles International Airport in 1999 in the so-called Millennium Plot. Meskini was able to use the stolen information and open bank accounts in New York City and Boston.

In order to protect our homeland and protect the good credit and reputations of hard-working Americans, the time for strong legislation cracking down on identity theft is now.

And I want to thank the Chairman for oversight of these two bills pending before us and urge my colleagues to support the strong and important legislation.

Mr. COBLE. I thank the gentleman.

Permit me to say a word prior to introducing our witnesses. Folks, there is nothing that annoys me any more severely than to see unscrupulous, dishonest persons benefiting and becoming unjustly enriched at the expense of innocent third parties. And this is what happens when this identity theft wheel begins to turn.

I think we have two good bills here. I am a cosponsor of Mr. Scott's bill. I told Bobby when I signed on, I said, "I like the bill, but I am little uneasy about the price tag." but he knows that price tags bother me generally.

But I think you and Mr. Schiff and Mr. Carter have done a good job as well.

I am pleased we are here today and I appreciate the interest as evidenced by the others in the hearing room.

Our first witness is Timothy Coleman. Mr. Coleman serves as counsel to Assistant Attorney General Christopher Wray of the Criminal Division of the U.S. Department of Justice where he advises the AAG on corporate fraud and other white-collar crime issues and works closely with the Department of Fraud section, the Enron Task Force and the President's Corporate Fraud Task Force.

Mr. Coleman served for 6 years as Assistant U.S. Attorney in the Southern District of New York and was a member of that office's Securities and Commodities Fraud Task Force. He is a 1990 graduate of Georgetown Law School. Prior to entering Government

service, he was in private practice at Cravath, Swaine & Moore in New York.

Our next witness is here today on behalf of the U.S. Secret Service. Mr. Larry Johnson serves as a special agent in charge for the Secret Service Criminal Investigative Division. He is responsible for the oversight of the Secret Service's criminal investigations, both domestic and overseas, which manages the electronic crime programs and initiatives, including the specialized training of agents in computer forensics and the development and implementation of the Secret Service's Electronic Crimes Task Force.

Our third witness, Mr. Robert Ryan is a senior director of TransUnion responsible for monitoring Federal and State legislation impacting TransUnion. Mr. Ryan currently serves on the Government Relations Working Group of the Consumer Data Industry Association, on the Board of Directors of the Coalition For Sensible Public Records Access, on the Advisory Board of the Information Policy Institute and on the Technology Policy Committee of the U.S. Chamber of Commerce.

Mr. Ryan received his Bachelor of Science Degree in Psychology from Loyola university in Chicago and completed the Executive Education Program at the University of Michigan in 1996. Mr. Ryan has also served in the U.S. Army Reserve, rising to the rank of captain.

And he joined TransUnion in 1971 as a consumer relations manager and has held numerous positions during his tenure, most recently as director of product development and management.

Our final witness representing the Fraternal Order of Police, properly known on the Hill as FOP—I assume Mr. Cannon, you will regard that as a complimentary term. Mr. Cannon is retired from the Washington, D.C., Metropolitan Police Department and currently inspector with the U.S. Mint Police. He is the current State Lodge President of the District of Columbia Lodge Number One of the Fraternal Order of Police and also serves as the chairman of the Federal Officers Committee.

Mr. Cannon, we appreciate your having responded at the last minute. Another one of our witnesses couldn't be here, and you agreed to fill in, and we appreciate that.

Good to have all of you with us. We have your written statements. Gentlemen, as we have told you, we have asked you before, and I want to reiterate this, if you can confine your statements to the 5-minute rule, we would be appreciative. We have hogs to slop and cows to juice around here, as we say in the rural South, and I am sure you all do as well. Now your warning will be that red light that will appear in the monitor in front of you. When the red light illuminates, you know you are in trouble with Mr. Scott and me. But if you could confine your statement to 5 minutes, we would be appreciative.

And Mr. Coleman, we will begin with you.

STATEMENT OF TIMOTHY COLEMAN, COUNSEL TO THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. COLEMAN. Good morning. Mr. Chairman and distinguished Members of the Subcommittee, thank you for inviting me to testify

on behalf of the Department of Justice on legislation that will help us deal more effectively with the important issue of identity theft.

Identity theft is one of the most widespread and growing types of criminal activity in the United States today. Millions upon millions of Americans have had their identities hijacked and used for criminal purposes. Already this morning, several Members of this Subcommittee have cited some of the statistics showing the magnitude of this problem, so I will just mention a couple more.

In 2002, nearly 10 million Americans were victims of identity theft. Over the past 3 years, the number of identity theft complaints has tripled. And the most recent statistic on the volume of identity theft cases is really staggering: As of December of last year, 2003, the Federal Trade Commission was receiving an average of 5,200 calls every week on its Identity Theft Telephone Hotline and another 800 complaints every week over the Internet.

Mr. Chairman, the numbers don't tell the whole story. Like Representative Schiff, as a Federal prosecutor, I have had a number of opportunities to witness first-hand the damage that identity thieves wreak on their victims, victims who are innocent and hard-working Americans, victims who have to suffer through the nightmare of having their credit and their good names ruined, victims who are forced to spend untold hours trying to repair their credit history and get their good names back.

Ever since the enactment of the Identity Theft and Assumption Deterrence Act in 1998, the Department of Justice has coordinated a nationwide, Federal, State and local law enforcement effort to combat this problem. For example, in 2002, the Attorney General announced a nationwide sweep of Federal identity theft prosecutions that involved 24 separate U.S. attorneys offices in 24 judicial districts around the country. We joined with the Secret Service, the Postal Inspection Service, the Federal Trade Commission and other agencies to sponsor a series of 11 regional seminars to train State and local law enforcement agents on identity theft, and we are continuing to assist other law enforcement agencies to further their efforts and ours in attacking this problem.

I am pleased to testify today in strong support of H.R. 1731, the "Identity Theft Penalty Enhancement Act." H.R. 1731 builds on and strengthens the important identity theft legislation that was enacted by Congress in 1998. Now that legislation, which is codified at 18 U.S.C. 1028(a)7, is one of the most important weapons in the arsenal of every Federal prosecutor, but we need more firepower on the front lines to combat the continuing problem of identity theft.

Let me extend the Department's gratitude to you, Mr. Chairman, and to Representative Carter for your leadership on this issue and for your prompt action on this legislation. We strongly support this bill, and we urge its swift enactment.

With the benefit of 6 years of experience under the 1998 legislation, H.R. 1731 includes targeted enhancements to existing law that would arm Federal prosecutors to fight identity theft more effectively. The bill would accomplish three principal and very important goals. Number one, it would define a class of offenses as aggravated identity theft, which would include the most serious and harmful forms of this activity.

Second, it would provide for more severe penalties in cases of identity theft, resulting in sentences that are more appropriate to the egregious nature of these cases and act as a more effective deterrent to would-be identity thieves.

And third, it would simplify and streamline the proof requirements for cases that are defined as aggravated identity theft, which sometimes have been very difficult to prosecute under the 1998 legislation. The Department strongly supports those enhancements. They would enable us to ensure that the most serious cases of identity theft are prosecuted effectively and punished appropriately and would enable us to work more effectively with our law enforcement and regulatory partners to reduce the incidents of identity theft.

That concludes my prepared remarks, and I will be pleased to answer any questions that the Members of the Subcommittee may have.

[The prepared statement of Mr. Coleman follows:]

PREPARED STATEMENT OF TIMOTHY COLEMAN

Mr. Chairman and distinguished Members of the Subcommittee, I am pleased to testify on behalf of the Department of Justice on the topic of identity theft. As Counsel to Assistant Attorney General (AAG) Christopher Wray in the Criminal Division at the Department of Justice, I advise the AAG on white collar crime issues, including identity theft. Previously, I worked for 6 years as an Assistant U.S. Attorney in the Southern District of New York, where I prosecuted dozens of cases of identity theft and other white collar crimes. As a federal prosecutor, I have had many opportunities to witness, first-hand, the damage that identity thieves wreak on their victims. Identity theft is one of the fastest growing crimes in the United States today. According to a survey conducted for the Federal Trade Commission (FTC) in 2003, nearly 10 million Americans had become victims of identity theft in the preceding year. Identity theft complaints to the FTC have nearly tripled in the past three years, from 86,212 complaints in 2001 to 214,905 complaints in 2003. Identity theft now accounts for 42 percent of all consumer complaints that the FTC receives—more than any other category of consumer fraud. I understand that as of December 2003, the FTC was receiving a weekly average of 5,200 calls on its identity theft telephone hotline, and another 800 complaints of identity theft over the Internet.

Additional data gathered by the General Accounting Office (GAO) paint a similar picture. In March 2002, the Government Accounting Office completed a report in which it concluded that all available sources of information confirm that "the prevalence of identity theft is growing" and that the monetary losses to industry from identity theft continue to mount. Numbers, however, do not tell the whole story. Identity theft inflicts substantial damage, not only on the economy, but also on hardworking Americans, who must expend the effort to undo the damage done to their credit records and their good names.

H.R. 1731

Let me first turn to H.R. 1731, the "Identity Theft Penalty Enhancement Act." I am pleased to testify in strong support of this important legislation. The Department first endorsed the approach of this legislation in 2002, as part of a two-pronged initiative to combat identity theft. The first prong was a coordinated, nationwide "sweep" to prosecute cases involving identity theft. This sweep resulted in 73 criminal prosecutions against 134 individuals in 24 judicial districts. The underlying criminal violations involved in these cases run the gamut from credit card fraud to theft of employee benefits to murder. These cases were the result of the close and ongoing cooperation among federal, state, and local law enforcement agencies, including the Federal Trade Commission (FTC), the Secret Service, the Postal Inspection Service, the FBI, the Office of the Inspector General of the Social Security Administration, the IRS's Criminal Investigation Division, as well as a range of state and local agencies.

Since that sweep, United States Attorneys' Offices across the country have continued their aggressive pursuit of identity theft cases. Acting through an interagency working group on identity theft, the Department has worked hard to coordinate enforcement efforts in this area. The FTC, working with the Secret Service, has pro-

vided invaluable assistance in developing an identity theft case referral program that helps in identifying significant cases that warrant further investigation.

At the same time, it is clear that the sentencing of identity theft offenders can be widely disparate. For example, one variety of identity theft that United States Attorneys' Offices are actively prosecuting are so-called "phishing" schemes—the use of emails and websites designed to look like those of legitimate companies' websites and emails in order to persuade people to disclose their personal or financial data. In some cases, where prosecutors can trace victim losses to the operation of the "phishing" scheme, they may be able to obtain more substantial sentences. If it is not possible to trace those losses, however, convicted defendants in phishing schemes may receive little or no imprisonment. In one case, which was prosecuted in the Western District of Washington, the defendant, despite having conducted a phishing scheme in which he masqueraded as the Microsoft Network (MSN), received only a sentence of probation.

The second prong of the Department's initiative was to strongly endorse legislation to enhance substantially the penalties for identity theft. Accordingly, in 2002, the Attorney General and Senator Feinstein jointly announced the outline of the legislation that is before you today. H.R. 1731, would greatly help to ensure that the Department has the tools it needs to prosecute effectively, and punish appropriately, the most serious forms of identity theft.

H.R. 1731 builds upon, and strengthens, the important identity theft legislation enacted by the Congress in 1998. The current federal identity theft statute is codified at 18 U.S.C. § 1028(a)(7). That provision makes it unlawful to "knowingly transfer[] or use[], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law," provided that the identification document in question was, or appears to be, issued by the United States or that the offense involved the use of the mails or affected interstate or foreign commerce. The existing statute has a sweeping substantive breadth that reaches all identity thefts that have a federal interest—even those involving State law felonies. This breadth makes it an essential element of the federal criminal code and an important weapon in the arsenal of every federal prosecutor. However, and precisely because of its breadth, the existing statute groups a large and disparate variety of misconduct into a single category. For the same reason, it also imposes across-the-board proof requirements that may be unduly restrictive in certain serious cases of identity theft.

Section 2 of H.R. 1731 addresses these concerns by proposing a new section 1028A to the criminal code. Section 1028A would define a class of "aggravated identity theft" that includes the most serious and harmful forms of this pernicious practice. The penalties for this newly defined crime of "aggravated identity theft" are significantly enhanced as compared to existing law, and the proof requirements are simplified.

In defining "aggravated identity theft," section 1028A—like the existing statute—uses the concept of predicate offenses. That is, identity theft generally is not committed for the sheer thrill of impersonation; it is almost always done for the purpose of committing another state or federal offense. Under H.R. 1731, the "aggravated" forms of identity theft are defined by the nature of the predicate offense, and include all of the most serious predicate offenses, as set forth in proposed section 1028A, subsections (a)(2) and (c). Thus, anyone who uses another person's identity to commit one of the enumerated serious predicate offenses will be guilty of "aggravated identity theft." Because virtually all of the most serious forms of identity theft involve predicate criminal activity that is covered by federal law—for example, bank fraud, wire fraud and mail fraud—H.R. 1731 does not include any State law predicate crimes in its definition of "aggravated identity theft." Compared to the general federal identity theft statute, H.R. 1731 applies to a focused and narrower set of predicate offenses.

In prescribing the penalties for this new offense, H.R. 1731 does not rely upon the Sentencing Commission or the Sentencing Guidelines. This approach is the most sensible one in light of the unusual nature of identity theft—it is an entirely derivative offense, in that it is virtually always committed in connection with some other crime. The Sentencing Guidelines, however, are generally designed and intended to be "charge-neutral:" in other words, the sentence depends on the underlying "relevant conduct" and not on the particular offense charged in the indictment. Thus, the Guidelines will generally ignore the fact that two offenses have been charged (a derivative offense and a predicate offense); the same sentence would be imposed in such a case as would be imposed even if only the predicate offense had been charged. Consequently, application of the Guidelines would mean that there would be virtually no practical advantage to charging the derivative criminal offense. Pros-

ecutors would have to charge more facts, and prove more facts, without obtaining any additional punishment.

H.R. 1731 avoids this problem through the structure of its penalty scheme. That scheme is modeled on the one used in 18 U.S.C. Section 924(c). That provision prohibits another derivative offense, using or carrying a firearm during and in relation to a crime of violence or a drug trafficking crime. Because an underlying predicate crime must be proved—either a crime of violence or a drug trafficking crime—application of the Guidelines would have collapsed the sentencing for the § 924(c) offense together with the underlying predicate offense. Section 924(c) avoids this by instead providing for an additional prescribed term of imprisonment over and above that imposed on the underlying offense. Because "aggravated identity theft" is unusual in that it is a derivative offense, like the conduct prohibited by § 924(c), a similar approach makes eminent sense here.

Accordingly, H.R. 1731 provides that, if a person commits aggravated identity theft by stealing someone's identity in order to commit a serious federal predicate offense, that person will be sentenced to an additional two years' imprisonment over and above the sentence for the underlying offense, as set forth in proposed section 1028A, subsections (a)(1) and (b)(2). If the predicate offense is a terrorism offense, the additional punishment is increased to five years, as set forth in the same proposed sections. H.R. 1731, however, properly departs from the § 924(c) model in one critical respect. In 1993, the Supreme Court held, in the case of *Deal* v. *United States*, 508 U.S. 129, that multiple counts under § 924(c) that are charged in the same indictment must run consecutively to each other. This mandatory, cumulative "stacking" of sentences, if applied here, could result in unduly severe and inflexible sentences. H.R. 1731 thus leaves it to the discretion of the sentencing judge whether to run consecutively or concurrently any multiple counts of aggravated identity theft that are sentenced at the same time, as set forth in proposed section 1028A, subsection (b)(4). In order to avoid unwarranted disparities in the exercise of this discretion, the Sentencing Commission is explicitly authorized to issue guidance concerning whether and to what extent such multiple sentences should be concurrent or consecutive. Id.

H.R. 1731 would also substantially simplify the proof requirements for "aggravated identity theft" compared to the current identity theft statute, 18 U.S.C. § 1028(a)(7). Section 1028(a)(7) contains multiple mental-state elements. In addition to proving all of the elements of the predicate crime (including the scienter element), prosecutors also must establish that the defendant "knowingly" transferred or used the identification "with the intent to commit" a federal or state crime. H.R. 1731 would streamline the proof for "aggravated identity theft," by requiring proof of only that level of scienter that is already required by the underlying predicate offense and the knowing use of another's identity. Moreover, because "aggravated identity theft" is defined with reference only to federal predicate offenses, there is no need for any additional proof of a federal jurisdictional connection. Accordingly, the additional federal jurisdictional showing required under § 1028(a)(7) is properly not carried over into this new offense.

This new offense defined by section 2, with its streamlined proof requirements and its enhanced penalty structure, will enable the Department to ensure significant identity theft crimes are effectively prosecuted and properly punished.

In addition to enacting a new offense of "aggravated identity theft," H.R. 1731 strengthens the existing 1998 identity theft law in multiple ways. Section 3 of the bill closes several gaps in the coverage of the existing identity theft prohibition (18 U.S.C. § 1028(a)(7)) and increases the penalties for certain violations of that section. As currently drafted, section 1028(a)(7) punishes anyone who "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet" any violation of Federal law or any State or local felony. This bill would amend this provision to prohibit, not just the "transfer or use" of someone else's identity information, but also the possession of such information with the requisite criminal intent.

The bill would also add language to this provision that would extend its coverage to those criminals who steal someone's identity "in connection with" another crime. The bill also amends section 1028(a)(7) to increase from three to five years the maximum term of imprisonment for ordinary identity theft and for possession of false identification documents. Lastly, section 3 of the bill would amend section 1028(b)(4) to impose a higher maximum penalty for identity theft used to facilitate acts of domestic terrorism. In doing so, section 3 builds upon the USA Patriot Act's definition of "domestic terrorism" and authorizes a 25-year maximum penalty for identity theft committed to facilitate an act of domestic terrorism.

I understand that the Subcommittee is reviewing proposed additions to H.R. 1731 that relate to issues raised by the Office of the Inspector General of the Social Secu-

rity Administration. These proposals would add sections 371 and 641 of Title 18 and section 1011 of Title 42 to the list of predicate offenses for aggravated identity theft, and would clarify the definition of the term "value" in section 641 of Title 18. With only one exception, the Department has no objection to those proposals. With respect to the inclusion of 18 U.S.C. § 371, the Department believes that it would be more consistent with the intent of this legislation to limit the inclusion of section 371 to conspiracies to commit any of the other substantive offenses listed in section 2 of the bill. Without this limitation, the addition of section 371 would allow application of the aggravated identity theft offense to any conspiracy covered by section 371, including conspiracies to violate any offense against the United States (even misdemeanors). This, in our view, would expand the reach of the enhancement considerably beyond what the Attorney General and the Administration have endorsed, and what we believe necessary to address the most serious identity theft offenses.

Let me extend the Department's gratitude to you, Mr. Chairman, and Representative Carter for your leadership on this issue and for your prompt action on this legislation. We strongly support this bill and urge its swift enactment.

H.R. 3693

I also want to address H.R. 3693, the "Identity Theft Investigation and Prosecution Act of 2003," which would authorize the appropriation of $100,000,000 for the investigation and prosecution of identity theft and related credit card and other fraud cases. I want to express my appreciation to Representative Scott and the cosponsors of this bill for their interest in ensuring that federal law enforcement can effectively pursue identity thieves. At the same time, I should note that we believe that the Administration's budget request is sufficient for the Department and other law enforcement agencies to continue their vigorous pursuit of identity theft.

That concludes my prepared remarks. At this time, I would be pleased to answer any questions you may have.

Mr. COBLE. Thank you Mr. Coleman, and you beat the 5-minute mark.

Mr. Johnson, you are recognized for 5 minutes.

STATEMENT OF LARRY D. JOHNSON, SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, UNITED STATES SECRET SERVICE

Mr. JOHNSON. Good morning, Mr. Chairman, Ranking Member Scott and Ranking Member Conyers and distinguished Members of the Subcommittee on Crime, Terrorism, and Homeland Security. Thank you for inviting me to testify on the subject of identity theft and the penalty enhancement act and the role the Secret Service has in these investigations.

As original guardian of our Nation's financial payment systems, the Secret Service has a long history of protecting American consumers and industry from financial fraud. With the passage of new Federal laws in 1982 and 1984, the Secret Service has provided primary authority for the investigation of access device fraud, including debit card and credit card fraud and parallel authority with other law enforcement agencies in identity crime cases.

In recent years, the combination of the information revolution, the effects of globalization and the rise of international terrorism have caused the investigative mission of the Secret Service to evolve dramatically. Explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes.

Our efforts to detect, investigate and prevent financial crimes are aggressive, innovative and comprehensive. As you are aware, this Congress is currently considering legislation that establishes in-

creased penalties for aggravated identity theft, that is, identity theft committed during and in relation to certain specific felonies.

H.R. 1731 and S. 153 provide for an additional 2 years of imprisonment for identity crime not to be served concurrently to the punishment associated with other related felonies and 5 years imprisonment if at least one of the related felonies is associated with terrorism. Additionally, the legislation prohibits the imposition of probation.

While this particular legislation cannot be expected to completely suppress identity theft, it does recognize the impact theft has on consumers and the need to punish those engaged in criminal activity for personal or financial gain.

The United States Secret Service believes this legislation has merit as it is an additional tool that law enforcement can utilize to the fullest extent in protecting our country's critical and financial infrastructure and citizens of the United States.

After 138 years in the Treasury Department, the Secret Service was transferred last year to the Department of Homeland Security with all our personnel, resources and investigative jurisdictions and responsibilities. Today, those jurisdictions and responsibilities require us to be involved in the investigation of traditional financial crimes as well as identity crimes and a wide range of electronic and high-tech crimes.

Identity theft criminals seek the personal identifiers generally required to obtain goods and services on credit, such as Social Security numbers, names and dates of birth. Identity crime involves the theft or misuse of an individual's financial identifiers, such as credit card numbers, bank account numbers and personal identification numbers.

With the proliferation of computers and the increase of the Internet, high-tech identity criminals begin to obtain information from company databases and Web sites. In some cases, the information obtained is in the public domain while, in others, it is proprietary and is obtained by means of computer intrusion or means of deception such as Web spoofing or phishing.

It has been our experience that criminal groups involved in these types of crime routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies who are first responders to their criminal activities.

By working closely with other Federal, State, local law enforcement agencies as well as international police agencies, we are able to provide a comprehensive network of intelligence-sharing, resource-sharing and technical expertise that bridges judicial boundaries. The Secret Service Electronic Crimes Task Force Program bridges the gap between conventional cyber-crimes investigations and the larger picture of critical infrastructure protection.

Secret Service efforts to combat cyber-based assaults that target information and communication systems supporting the financial sector are a large part and more comprehensive critical infrastructure protection and counterterrorism strategy. It is through our hard work in these areas of financial and electronic crimes that we have developed particular expertise in the investigation of credit card fraud, identity theft, check fraud, cyber crime, false identifica-

tion fraud, computer intrusions, bank fraud and telecommunications fraud.

While our task forces do not focus extensively on identity crime, we recognize that stolen identifiers are often a central component of other electronic or financial crimes. Subsequently, our task forces have devoted considerable time and resources to the issue of identity crime.

Mr. Chairman, that concludes my prepared statement.

[The prepared statement of Mr. Johnson follows:]

PREPARED STATEMENT OF LARRY D. JOHNSON

Good afternoon, Mr. Chairman. I would like to thank you, as well as the distinguished Ranking Member, Mr. Scott, and the other members of the subcommittee for providing an opportunity to discuss the subject of identity crime, and the role of the Secret Service in these investigations.

Identity crime is the theft or misuse of an individual's personal or financial identifiers in order to gain something of value or to facilitate other criminal activity. Types of identity crime include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud, and passport/visa fraud. Equally as important is that identity crimes are used to facilitate and fund violent crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud, and terrorism. Identity crimes provide the anonymity for criminals to operate undetected and, along with untraceable financing, to fund such criminal endeavors.

It is through our work in the areas of financial and electronic crime that we have developed particular expertise in the investigation of credit card fraud, identity theft, check fraud, cyber crime, false identification fraud, computer intrusions, bank fraud, and telecommunications fraud. Secret Service investigations typically focus on organized criminal groups, both domestic and transnational.

As you are aware, Mr. Chairman, the House and the Senate are each considering legislation that establishes increased penalties for aggravated identity theft—that is, identity theft committed during and in relation to certain specified felonies. H.R. 1731 and S. 153 provide for an additional two years imprisonment for the identity crime, not to be served concurrently to the punishment associated with the other related felony or felonies, and five years imprisonment if at least one of the related felonies is associated with terrorism. Additionally, the legislation prohibits the imposition of probation.

While we are all aware that no legislation can be expected to completely suppress identity theft, these efforts recognize the impact identity theft has on consumers and the need to punish those engaging in criminal activity for personal or financial gain. The Secret Service believes this legislation has merit as an additional tool that law enforcement can utilize in protecting our commercial and financial infrastructures and the citizens of the United States.

In addition to providing the highest level of physical protection to our nation's leaders, the Secret Service exercises broad investigative jurisdiction over a wide variety of financial crimes. As the original guardian of our Nation's financial payment systems, the Secret Service has a long history of protecting American consumers and industry from financial fraud. With the passage of legislation in 1982 and 1984, the Secret Service was provided authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases. In recent years, the combination of the information revolution, the effects of globalization and the rise of international terrorism have caused the investigative mission of the Secret Service to evolve dramatically.

After 138 years in the Treasury Department, the Secret Service was transferred in 2003 to the Department of Homeland Security with all of our personnel, resources and investigative jurisdictions and responsibilities. Today, those jurisdictions and responsibilities require us to be involved in the investigation of traditional financial crimes as well as identity crimes and a wide range of electronic and high-tech crimes.

The burgeoning use of the Internet and advanced technology have intensified competition within the financial sector. With lower costs of information-processing, legitimate companies have found it profitable to specialize in data mining, data warehousing and information brokerage. Information collection has become a common byproduct of newly-emerging e-commerce. Internet purchases, credit card sales,

and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products.

All of this has led to a new measure of growth within the direct marketing industry that promotes the buying and selling of personal information. In today's markets, consumers routinely provide personal and financial identifiers to companies engaged in business on the Internet. They may not realize that the information they provide in credit card applications, loan applications, or with merchants they patronize are valuable commodities in this new age of information trading. Consumers may be even less aware of the illegitimate uses to which this information can be put. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders. But legitimate business can provide a first line of defense against identity crime by safeguarding the information it collects. Such efforts can significantly limit the opportunities for identity crime, even while not eliminating its occurrence altogether.

According to statistics compiled by the Federal Trade Commission for calendar year 2003, 42% of the 516,740 victim complaints reported involved at least one type of identity crime. The complaints were broken down as follows *(note that some complaints involved more than one of the listed activities):*

- **33%** of complaints involved credit card fraud—i.e., someone either opened up a credit card account in the victim's name or "took over" the victim's existing credit card account;
- **21%** of complaints involved the activation of telephone, cellular, or other utility service in the victim's name;
- **17%** of complaints involved bank accounts that had been opened in the victim's name, and/or fraudulent checks had been negotiated in the victim's name;
- **11%** of complaints involved employment-related fraud;
- **8%** of complaints involved government documents/benefits fraud;
- **6%** of complaints involved consumer loans or mortgages that were obtained in the victim's name; and
- **19%** of complaints involved some type of miscellaneous fraud, such as medical, bankruptcy and securities fraud.

Although financial crimes are often referred to as "white collar" by some, this characterization can be misleading. The perpetrators of such crimes are increasingly diverse and today include both domestic and international organized criminal groups, street gangs, convicted felons and terrorists.

These criminals seek the personal identifiers generally required to obtain goods and services on credit such as social security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers and personal identification numbers.

The methods of identity criminals vary. "Low tech" identity criminals obtain personal and financial identifiers by going through commercial and residential trash, a practice known as "dumpster diving." The theft of wallets, purses and mail is also widespread practice employed by both individuals and organized groups.

With the proliferation of computers and increased use of the Internet, "high tech" identity criminals can obtain information from company databases and web sites. In some cases, the information obtained is in the public domain while in others it is proprietary and is obtained by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a utility billing center, financial institution, medical office, or government agency. The collusive employee will access the proprietary data base, copy or download the information, and remove it from the workplace either electronically or simply by walking it out.

Once the criminal has obtained the proprietary information, it can be exploited by creating false "breeder documents" such as a birth certificate or social security card. These documents are then used to obtain genuine, albeit false, identification such as a driver's license and passport. Now the criminal is ready to use the illegally obtained personal identification to apply for credit cards, consumer loans or to establish bank accounts, leading to the laundering of stolen or counterfeit checks or to conduct a check-kiting scheme. Our own investigations have frequently involved the targeting of organized criminal groups that are engaged in financial

crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal identifiers to further their other criminal activity.

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as the first responders. By working closely with other federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that fall within the investigative jurisdiction of the Secret Service.

Members of these task forces, which include representatives from local and state law enforcement, prosecutors' offices, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes. The value of this crime fighting and crime prevention model has been recognized by this subcommittee and by Congress as a whole, directing the Secret Service (pursuant to the USA PATRIOT Act of 2001) to expand our electronic crime task forces to cities and regions across the country. Recently, four new Electronic Crimes Task Forces (ECTFs) were established in Dallas, Houston, Columbia (S.C.) and Cleveland, and additional task forces will be added this year.

The Secret Service is actively involved with a number of government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of Justice. This group, which is comprised of federal, state, and local law enforcement agencies, regulatory agencies, and professional organizations, meets regularly to discuss and coordinate investigative and prosecutorial strategies as well as consumer education programs.

In a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission (FTC) and the International Association of Chiefs of Police (IACP), we are hosting Identity Crime Training Seminars for law enforcement officers. In the last two years we have held seminars for officers in Chicago, Dallas, San Francisco, Las Vegas, Des Moines, Washington D.C., Phoenix, New York, Seattle, San Antonio, Providence and Orlando. In the coming months, we have training seminars scheduled in Raleigh, Buffalo and Denver. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

Operation Direct Action (ODA), an initiative led by the Secret Service, targets organized criminal groups that are committing large scale financial fraud, specifically credit card "bust out" schemes, which may impact our nation's financial infrastructure. A credit card "bust out" scheme is a type of fraud where a criminal obtains multiple credit card accounts and manipulates the lines of credit that are established with each card. The criminal makes payments with convenience checks issued by another card or with non-sufficient funds checks drawn on one of his or her many bank accounts. The criminal is taking advantage of the lag time that will occur between when his accounts will be credited with the payment and when the issuing banks determine that the checks were bad.

While our task forces do not focus exclusively on identity crime, we recognize that stolen identifiers are often a central component of other electronic or financial crimes. Consequently, our task forces devote considerable time and resources to the issue of identity crime.

Another important component of the Secret Service's preventative and investigative efforts has been to increase awareness of issues related to financial crime investigations in general, and of identity crime specifically, both in the law enforcement community and the general public. The Secret Service has tried to educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives.

For example, criminals increasingly employ technology as a means of communication, a tool for theft and extortion, and a repository for incriminating information. As a result, the investigation of all types of criminal activity, including identity crime, now routinely involves the seizure and analysis of electronic evidence. In fact, so critical was the need for basic training in this regard that the Secret Service joined forces with the IACP and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is de-

signed for the first responder, line officer and detective alike. This guide assists law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies.

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 distributed 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.

In addition, we have just completed the Identity Crime Video/CD-ROM which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to police officers at their roll call meetings which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the FTC and the IACP. To date, over 40,000 Identity Crime CD-ROMs have been distributed to law enforcement departments and agencies across the United States.

The Secret Service has also assigned a special agent to the FTC as a liaison to support all aspects of the Commission's program to encourage the use of the Identity Theft Data Clearinghouse as a law enforcement tool. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of "consumer awareness" initiatives regarding identity theft.

It is important to recognize that public education efforts can only go so far in combating the growth of identity crime. Because social security numbers, in conjunction with other personal and financial identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim.

Mr. Chairman, it is apparent that identity crime must be combated on all fronts, from the officer who receives a victim's complaint, to the detective or Special Agent investigating an organized identity theft ring. The Secret Service has already undertaken a number of initiatives aimed at increasing awareness and providing the training necessary to address these issues, but those of us in the law enforcement and consumer protection communities need to continue to reach out to an even larger audience. We need to continue to approach these investigations with a coordinated effort—this is central to providing a consistent level of vigilance and addressing investigations that are multi-jurisdictional while avoiding duplication of effort. With the support of this subcommittee, the Secret Service will continue to work to protect the nation's consumers from identity theft criminals.

Mr. Chairman, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

Mr. COBLE. I thank the gentleman.

And we have been joined by the distinguished gentleman from Texas, Mr. Carter, who, along with Mr. Schiff, sponsors H.R. 1731. Good to have you with us, Mr. Carter.

Mr. Ryan, you are recognized for 5 minutes.

STATEMENT OF ROBERT F. RYAN, SENIOR DIRECTOR, GOVERNMENT RELATIONS, TRANSUNION

Mr. RYAN. Good morning, Chairman Coble, Congressman Scott and Members of the Subcommittee.

My name is Bob Ryan, and I am Senior Director of Government Relations for TransUnion. We are a leading global provider of consumer report information, supported by 4,100 employees in 24 countries. I appreciate the opportunity to appear before you today

to discuss our role in assisting consumers and our business customers in preventing and remediating identity theft and additional steps that can be taken to fight identity theft.

Identity theft is a serious problem and TransUnion is part of the solution. Since the 1990's, when we developed the first application-fraud detection services for credit granters, we have been helping our business customers detect and avoid application fraud and thus reducing the number of consumers affected by identity theft.

In the mid-1980's, we were the first consumer reporting agency to develop special procedures to assist identity theft victims, including expedited dispute verification processes.

In the late 1980's, we developed the innovation of a security alert flag on credit reports to alert our customers to use extra caution in opening new accounts.

In 1992, we were the first consumer reporting agency to establish a special Fraud Victim Assistance Group within our organization that is solely dedicated to identity theft problems.

In 1997, we began immediate suppression of fraud related information on a consumer's file upon their presentation of a police report or other documentation confirming the fraud.

In March 2000, this process became an industry standard. Our identity-fraud specialists work with consumers, with industry and with Government agencies to remediate damaged credit files as quickly as possible and to take preventative steps that reduce further victimization and to cooperate with law enforcement authorities in their investigations and prosecutions of this crime.

Earlier this year, we introduced our latest service for business and Government agencies supporting both verification and authentication of an individual's identity. Our Fraud Management Platform service provides access to a large array of fraud-related information with analytics and technology to support businesses and agencies of all sizes.

Congress has also taken important steps recently with respect to identity theft. We applaud Congress for enacting last year, December of 2003, the Fair and Accurate Credit Transactions Act or the FACT Act, which makes permanent important national standards in the credit reporting system and includes a comprehensive set of provisions pertaining to identity theft, many of which I describe in my written statement.

Although the ink is barely dry on the FACT Act, let me offer six suggestions as to further steps that Congress, law enforcement and other holders of personal information can take to combat identity theft.

First, Congress should enact H.R. 1731 and H.R. 3693 to improve the weapons available to law enforcement to fight identity theft.

Second, in enacting new legislation, Congress should set uniform national standards in order to promote better consumer education and better implementation by those who must comply with new laws.

Third, in considering legislation which would restrict access to personal information held by Government agencies or in public records, Congress should provide for continued access for consumer reporting agencies such as TransUnion. Our continued access to this information strengthens the quality of identity verification and

authentication services that we are able to provide to business, Government and law enforcement.

Fourth, law enforcement's efforts to coordinate investigations and identity-theft databases should be encouraged.

Fifth, we would like to see a single Federal law enforcement agency become the principal issuer of identity theft reports to individuals who become victims. Unfortunately, forged identity theft reports are a problem today for credit reporting agencies. A standardized form, which the FTC has worked toward, but with appropriate safeguards against false claims will make it easier and simpler for victims to trigger their rights under the Fair Credit Reporting Act and will also allow consumer reporting agencies and financial institutions to verify the report.

Sixth and finally, we would like to see holders of personal information notify each individual when his or her personal information is improperly obtained by an unauthorized person resulting in or likely to result in identity theft. We think holders of personal information should work with one or more consumer reporting agencies in these cases to coordinate the posting of security alerts and to reimburse the agencies for the costs of supporting the consumer in posting the alerts.

At TransUnion, we are proud of our leadership in the development of processes and procedures to prevent and remediate identity theft.

Mr. Chairman and Members of the Subcommittee, I sincerely appreciate your invitation to testify today. We look forward to being part of the solution of this terrible crime and I would be pleased to answer any questions you have.

[The prepared statement of Mr. Ryan follows:]

PREPARED STATEMENT OF ROBERT RYAN

Statement of Robert Ryan,

Senior Director of Government Relations
TransUnion, LLC

Before the

Subcommittee on Crime, Terrorism and Homeland Security
Of the Judiciary Committee

HR 1731: The Identity Theft Penalty Enhancement Act
&
HR 3693: Identity Theft Investigations and Prosecution Act of 2003

March 23, 2004

Introduction

Good morning, Chairman Coble, Congressman Scott, and Members of the Subcommittee. My name is Robert Ryan, and I am Senior Director of Government Relations for TransUnion, LLC. TransUnion is a leading global provider of consumer report information supported by more than 4,100 employees in more than 24 countries worldwide. I appreciate the opportunity to appear before you today to discuss the role of TransUnion in the credit granting process and in assisting consumers and our business customers in preventing and remediating identity theft, and additional steps that can be taken to fight identity theft.

The Role of TransUnion in the Credit Granting Process

Consumer spending makes up approximately two-thirds of the U.S. gross domestic product. A critical component of this economic driver is the availability of consumer credit. Consumers in the United States have access to a wide variety of credit from a number of sources at extremely competitive prices. Consumers rely on the availability of credit for a variety of purposes, such as the purchase of homes, cars, education, and daily needs. In fact, there is approximately $7 trillion in outstanding mortgages and other consumer loans in the United States. There is no question that our economy would suffer if consumers could not easily access credit as they do today.

It is my pleasure to explain how TransUnion plays a critical role in the economic engine of credit availability. In sum, we provide the information necessary for lenders, regardless of where they are located, to make credit available to consumers all across the United States. In order for a lender to extend a loan to a consumer, the lender must evaluate the credit risks inherent in lending to that consumer. The proper evaluation of

the consumer's credit risks allows the lender to determine whether to provide credit to the consumer and at what price. We believe that the most accurate and predictive piece of information a lender can use in evaluating a consumer's credit risk is a consumer report (also commonly called a credit report). TransUnion is in the business of providing lenders with this critical information.

The Credit Reporting Process

In order to more fully understand TransUnion's role in the credit availability process, it is important to understand the credit reporting process itself. TransUnion is a national consumer reporting agency. We are a nationwide repository of consumer report information with files on approximately 200 million individuals in the United States. The information in our files generally consists of: (i) identification information (including social security numbers); (ii) credit history; (iii) public records (*e.g.* tax liens, judgments, etc.); and (iv) a list of entities that have received the consumer's credit report from us. It is also important to clarify what is not in a credit report. A TransUnion credit report does not include checking or savings account information, medical histories, purchases paid in full with cash or check, business accounts (unless the consumer is personally liable for the debt), criminal histories, or race, gender, religion, or national origin.

Most of the information in our files is provided to us voluntarily by a variety of sources. Although the Fair Credit Reporting Act (FCRA) does not require anyone to furnish information to consumer reporting agencies, or have any rules on the scope or nature of such information, the law does establish certain important guidelines for those who voluntarily furnish information to consumer reporting agencies. For example, furnishers must meet certain accuracy standards when providing information to consumer reporting agencies. Furnishers must also meet requirements ensuring that the information the furnishers have reported to consumer reporting agencies remains complete and accurate. Despite these legal obligations imposed on data furnishers, lenders and others participate in the credit reporting process due to the recognized value of complete and up-to-date credit reporting. In essence, if lenders want accurate, complete, and up-to-date information on which they are to base credit decisions, they must ensure a continuing supply of such data to consumer reporting agencies.

We take great pride in our ability to collect and disseminate credit report information. In fact, TransUnion receives and processes approximately 2 billion updates to consumers' credit files each month. However, we do not distribute credit reports to just anyone. Under the FCRA, we may not provide a credit report to anyone who does not certify to us that they have a permissible purpose for such information. This protection ensures that the distribution of credit reports is made only to those with a need for such information (*e.g.* granting credit).

The Role of TransUnion in Identity Theft Prevention and Remediation

TransUnion Is Part of the Solution

Identity theft is a serious problem and TransUnion is part of the solution. Since the 1980s, when TransUnion developed the first application fraud detection suite of services for credit grantors (our HAWK® products, introduced in 1983), we have recognized that fraud through identity theft is a problem for which we can be part of the solution. We have been helping our customers detect and avoid application fraud for over 20 years, thus reducing the number of consumers affected by identity theft. In the mid-1980s we were the first consumer reporting agency to initiate the development of special procedures to assist identity theft victims, including expedited dispute verification processes and the deletion of fraudulent information. In the late 1980s we developed the innovation of a "security alert" flag on credit reports, to alert our customers to use extra caution in opening new accounts.

In 1992, we were the first national consumer reporting agency to establish a special Fraud Victim Assistance group within our organization that is solely dedicated to identity theft problems. In 1997 we began immediate suppression, at the same time the dispute investigation process was initiated, of fraud-related information on a consumer's file upon their presentation of a police report or other documentation confirming the fraud. In March 2000, this process became an industry standard.

Our identity fraud specialists work with consumers, industry, and government agencies to remediate damaged credit files as quickly as possible, to take preventive steps that reduce further victimization, and to cooperate with law enforcement authorities in their investigations and prosecutions of this crime. As we explain on our web site, www.transunion.com, our process includes posting a security alert, opting the victim out of prescreening if the victim wishes, and notifying inquirers whose inquiries were due to fraud. We are proud to have played a leadership role in the development of processes that have become national standards today and expect to continue this leadership to combat this growing crime.

In terms of preventing identity theft, our most recent business-to-business offering to combat fraud is the Fraud Management Platform. The program provides convenient access to one of the most comprehensive sets of fraud-related databases ever assembled, along with cutting edge analytics and the decisioning technology to help our clients identify fraud. Our Fraud Management Platform gives businesses and government agencies of all sizes the ability to verify and authenticate customer information, allowing businesses and agencies to detect identity thieves more easily. In other words, businesses and government agencies will be better able to determine whether the identifying information submitted by an individual is accurate, and that the individual is actually who they claim to be. We would be happy to provide the Subcommittee more detailed information about any of our fraud-prevention services upon request.

The Importance of National Standards in Combating Identity Theft: The FACT Act of 2003

The Fair and Accurate Credit Transactions Act of 2003

As you know, on December 4, 2003, President Bush signed into law the Fair and Accurate Credit Transactions Act of 2003, or the FACT Act. We applaud Congress for enacting the FACT Act, which makes permanent important national standards in the credit reporting system, and includes a comprehensive set of provisions pertaining to identity theft. I am pleased to note that many of the identity theft provisions in the FACT Act are based on innovations that TransUnion and other consumer reporting agencies have developed to help consumers in the fight against identity theft.

A significant provision in the new law is a requirement to provide free credit report annually to consumers upon request. This new obligation springs from the idea that if the credit report is free there will be increased access to credit histories by more people, and that increased access will improve accuracy and reduce identity theft by encouraging individuals to regularly review their credit reports. There remains significant debate as to the validity of this logic since credit reports were always accessible for a modest fee (currently $9) and for many years all national consumer reporting agencies have provided free credit reports, upon request, to identity theft victims and to individuals who think there may be fraudulent information on their reports.

The new law also provides for three types of security alerts in credit reports—an initial alert (upon a good faith suspicion that the individual may be subject to identity theft), a "military" alert (for our men and women serving in the military away from home), and an extended alert (in cases of actual identity theft). As a general matter, certain users of consumer reports (*e.g.* creditors) are required to take steps to confirm a consumer's identity prior to extending credit when these alerts are present on credit reports. As I mentioned above, TransUnion was a pioneer in giving consumers the opportunity to place security alerts in their credit files.

The FACT Act also codifies what has been our industry's voluntary practice concerning the immediate blocking of information related to identity theft upon the consumer's providing us with an identity theft report—usually a police report. This practice is also known as "tradeline blocking." The national consumer reporting agencies are required to share information about security alerts and blocked data among themselves, so that a consumer's actions with one consumer reporting agency will flow to the others, and be reflected on their credit reports.

The FACT Act will also benefit consumers by requiring the Federal Trade Commission to develop a summary of consumer rights under the FCRA with respect to the procedures for remedying the effects of fraud or identity theft involving credit or other financial accounts or transactions. This provision is designed to assist identity theft victims in understanding the numerous tools at their disposal, such as the use of security alerts or tradeline blocking, to mitigate the harms of identity theft. Consumer reporting

agencies will provide a summary of these rights to any consumer who contacts them and expresses a belief that he or she is a victim of fraud or identity theft involving a financial transaction.

The FACT Act also requires a consumer reporting agency to provide a "heads up" to a user of credit reports if the user submits to a consumer reporting agency an address for a consumer that does not match an address in the consumer reporting agency's files. This provision is based on existing practices used by TransUnion to notify creditors and others that the consumer's address does not match one we have on file. This serves as another protection against identity theft, where the criminal may use a victim's identification information but the criminal's address in order to obtain credit or other goods or services. Under the FACT Act, the user of a credit report that contains such a notice of discrepancy will need to take certain steps to reduce the risk that the transaction is the result of identity theft.

The issue of data furnishers providing the consumer reporting agency information that has been identified as fraudulent by the consumer reporting agency, and has been "blocked" by the consumer reporting agency, has been addressed by the FACT Act in two ways. First, in certain circumstances, the law prohibits the sale to third parties of accounts on which the creditor has received a notice of identity theft from either the consumer directly, or from the consumer reporting agency. The intent is to prevent the fraudulent information from finding its way back onto the credit report in the form of a report from a third party collection agency. Second, the FACT Act prohibits data furnishers from providing information to a consumer reporting agency if the consumer provides them an identity theft report identifying the relevant information as resulting from identity theft, or if the furnishers are notified by a consumer reporting agency that an identity theft report has been filed with respect to such information.

Furnisher Obligations

Because the FACT Act makes permanent the national standards pertaining to data furnisher obligations, it removed the danger that state laws pertaining to furnisher obligations could have reduced the number of entities willing to provide information to consumer reporting agencies. Withdrawal of data furnishers from the system would result not only in a loss of the credit information they provide but would also result in the loss of the address updates they provide. TransUnion's database relies on addresses that are in active use by creditors in mailing monthly statements to their customers. The fact that most data furnishers today also provide us with the social security number of their customers allows us to bridge address changes and name variations that commonly occur in our society. Businesses and government agencies with a permissible purpose to obtain a consumer report rely on our robust national database of names, social security numbers, and up to date addresses for a variety of fraud prevention and identity authentication services. With less current identification or address information coming into the database, the performance of these services would suffer.

Reinvestigation Timeframes

In identity theft cases, the consumer reporting agency is tasked with sorting out accurate and inaccurate information about the consumer. This is a difficult process and, if not done properly, could affect not only the consumer's ability to obtain credit but the safety and soundness of our financial institutions. We were gratified that the FACT Act preserved the national standard for reinvestigation processes and timeframes. In this regard, identity theft victims in Pennsylvania will continue to be treated no differently than victims from California to Florida. As a nation, we cannot have any other result.

What More Can Be Done?

We recognize that despite our best efforts, and the enactment of the FACT Act, that more can be done to address identity theft. This hearing is to examine more broadly any additional steps that can be taken by Congress, by law enforcement, and by holders of individuals' personal information. Allow me to respectfully offer these thoughts:

Congress

Although Congress has provided for several laws pertaining to identity theft, identity thieves can operate with the belief that, in the event that their crimes are investigated and prosecuted, the criminal penalties are not so severe as to deter their actions. We believe more can be done to find, investigate, and prosecute identity thieves and to punish them more severely. Therefore, TransUnion strongly supports H.R. 1731, the Identity Theft Penalty Enhancement Act, introduced by Congressman Carter and Congressman Schiff, and H.R. 3693, introduced by Congressman Scott and Chairman Coble. Both of these bills deserve the bi-partisan support they have received. We believe that each of these bills, by stiffening criminal penalties for identity theft crimes and increasing the resources available to investigate such crimes, would provide key tools in our fight against identity theft.

I would also like to stress the advantages of national standards regarding the protection of personal information. Most major holders of personal information are nationwide institutions. Furthermore, in our age of technology, personal information flows rapidly across state borders to serve consumers quickly and accurately. Any new federal provisions pertaining to consumer information must establish a uniform national standard to enable better consumer education and more reliable implementation by persons covered by any new law.

In considering legislation to protect personal information held in public records (or other records held by government), Congress should remember that access to this information by legitimate companies (such as consumer reporting agencies governed by the FCRA) helps to combat identity theft. The reverse is also true—to the extent consumer reporting agencies, and other legitimate businesses servicing both government and industry, are denied access to complete personal information in government records, we are hindered in our ability to combat identity theft though services such as the Fraud

Management Platform, described above. Legislation restricting access to personal information should provide appropriate exemptions for these purposes.

Law Enforcement

Many law enforcement agencies, at many levels of government, are doing excellent work in aggregating information on identity theft in order to fight the crime and to assist victims. Federally, the Secret Service, the FBI, and the FTC all have databases of identity theft information that are shared with local law enforcement. The Attorneys General of California, and other states, have their own databases of identity theft cases. The financial crimes units of many major police departments in cities like Chicago, Los Angeles and New York also have their own databases of identity fraud cases. We applaud efforts to assist all levels of law enforcement to improve communications and information sharing, in order to enhance effective prosecution of these crimes. We believe that H.R. 1731 and H.R. 3693 will improve the weapons available to law enforcement in this regard.

Second, we support efforts to improve the ease with which identity theft victims can file identity theft reports, in a way that does not promote further fraud.[1] Today at TransUnion we regularly receive fraudulent or forged police reports—it's a common tactic of credit clinics used to attempt to have accurate information removed from credit histories. We would like to see true identity theft victims have access to a more uniform means of filing genuine identity theft reports, such as through a federal law enforcement agency like the U.S. Postal Inspection Service. These standardized reports would be of use to law enforcement investigations spanning multiple jurisdictions. Such reports would also be more readily verifiable by consumer reporting agencies, and thus cut back on credit clinic abuse of the consumer reporting system.

Holders of Personal Information

We believe that legislation is needed concerning breaches of the security of personally identifiable information. In the event that personally identifiable information is compromised and obtained by unauthorized persons, we believe the holder of that information should have several responsibilities: First, if the holder of the information has reason to believe that the personal information may be used to harm the consumer to whom the information pertains, the holder should notify each person whose personal information was exposed, and the holder should coordinate with at least one of the national consumer reporting agencies (such as TransUnion) to arrange for initial alerts to be posted on those individuals' credit reports. Second, the holder of the information

[1] The FACT Act defines an identity theft report, subject to further rulemaking by the Federal Trade Commission, as a report "that alleges identity theft, that that is a copy of an official, valid report filed by a consumer with an appropriate federal, state or local law enforcement agency, including the United States Postal Inspection Service, or such other government agency deemed appropriate by the Commission; and the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information if, in fact, the information in the report is false." 15 U.S.C. § 1681a(q)(4)

should have a duty to reimburse the consumer reporting agency for the costs of the postings of alerts and any subsequent file disclosures and reinvestigations.

Conclusion

At TransUnion, we are proud of our leadership in the development of processes and procedures to prevent and remediate identity theft. We applaud the 108th Congress for enacting the FACT Act, creating important new national standards that will help remediate identity theft. We are gratified that many of the provisions in that bill were based on credit reporting industry standards that TransUnion helped put in place. We also support both the intent and the substance of the two bills before this Subcommittee today, establishing stiffer penalties for aggravated identity theft, and to provide additional resources to law enforcement for combating this crime. We appreciate the opportunity to present our suggestions for additional measures which this Subcommittee may wish to consider.

Mr. Chairman, Congressman Scott, and members of the Subcommittee, I sincerely appreciate your invitation to testify today on identity theft. TransUnion looks forward to continuing to be part of the solution to this terrible crime.

Mr. COBLE. Mr. Cannon.

STATEMENT OF LOUIS P. CANNON, STATE LODGE PRESIDENT, DISTRICT OF COLUMBIA, LODGE NUMBER ONE, FRATERNAL ORDER OF POLICE AND CHAIRMAN, FEDERAL OFFICERS COMMITTEE

Mr. CANNON. Good morning, Mr. Chairman, Ranking Member Scott and Ranking Member Conyers, distinguished Members, Mr. Schiff and Mr. Carter.

I am a 30-year law-enforcement veteran, having served with the Metropolitan Police Department of Washington, D.C. and currently holding the rank of inspector with the United States Mint Police.

Nationally, the FOP is the Nation's largest law enforcement organization, representing more than 311,000 rank and file law enforcement officers in every region of the country. I am here this morning at the request of Chuck Canterbury, National President to the FOP to discuss two pieces of legislation, H.R. 1731, the "Identity Theft Penalty Enhancement Act" and H.R. 3693, the "Identity Theft Investigation and Prosecution Act of 2003" and also give this Subcommittee the views of FOP on the rise of identity crimes in the United States.

The technology of the Information Age has allowed criminals to commit traditional crimes in new ways; identity theft is one such example. A criminal who obtains key pieces of personal information—Social Security, driver's license numbers, for example—can then commit fraud and other crimes by purchasing credit, merchandise and services in the name of the victim.

Identity theft is the fastest growing crime in the United States. The Federal Trade Commission found that complaints of identity theft increased 87 percent between 2001 and 2002, and over 161,000 complaints were received by the agency last year.

As cited by you, Mr. Chairman, the cost of these crimes is high. The FTC estimates the loss to businesses and financial institutions to be approximately $47.6 billion, and the cost to individual consumers is estimated to be approximately $5 billion.

The FOP is very pleased to have played a leadership role in the recent enactment of S. 1581, the "Identity Theft Victims Assistance Act," which was passed as a component of H.R. 2622, the "Fair and Accurate Credit Transactions Act" and signed into law in December of last year. This legislation gives law enforcement officers the tools to better investigate identity theft crimes by allowing victims to designate local law enforcement as their agent in obtaining business records, applications for credit, records of sales and other documents relating to ongoing fraud. Access to such records will greatly improve the speed and effectiveness of investigations into these types of crimes.

Without a court order, most creditors are unwilling to divulge information to law enforcement about open accounts because of liability concerns and a good-faith desire to protect the privacy rights of the account holder. The new law provides that a new business may not be held liable for any disclosure made in good faith to further prosecution of identity theft. This is a huge step forward for law enforcement because of the lack of timely information about the

fraudulent transaction delays the progress of the investigation and the chances of closing the case.

The nature of the crimes makes it difficult for local and State law enforcement to investigate these crimes effectively or even take a report. For example, a victim in South Carolina has his identity stolen while on vacation in Florida, and the information is used to buy merchandise in New Jersey. Where was the crime committed? South Carolina, where the victim resides? Florida where the information was stolen? Or the point of purchase in New Jersey? What if the fraudulent purchase was made online?

Now, the Congress has addressed one of the hurdles on the ability of law enforcement to collect the information it needs to investigate such crimes. We believe further Federal funding will enable us to aggressively investigate these cases and go after these criminals.

Legislation like H.R. 3693 offered by the Ranking Member and Chairman of this Committee would authorize $100 million to the Department of Justice for the investigation and prosecution of identity theft and identity fraud cases. The legislation does not restrict how that money might be used, allowing law enforcement to develop and fund its best approach, be it equipment, multi-jurisdictional task forces or grants to State and local agencies.

Similarly, Congress should consider enhancing the available penalties to identity criminals as contemplated by H.R. 1731.

I would like to thank the Subcommittee for asking me to appear today, and I would be happy to answer any questions you might have.

[The prepared statement of Mr. Cannon can be found in the Appendix.]

Mr. COBLE. Thanks to all of you for your testimony. Gentlemen, we impose the 5-minute rule against ourselves, so if you can keep your answers concise that will enable us to present more questions to you.

Mr. Coleman, H.R. 3369 proposes the Department of Justice be ultimately authorized $100 million to combat identity crime. Given the fact that identity theft is intertwined with so many other crimes, how do you envision that these funds will be utilized to address this problem, A? And B, did the President request funds to combat identity theft in his budget proposal?

Mr. COLEMAN. Mr. Chairman, the Department of Justice has been acting very aggressively against identity fraud for several years. As I mentioned earlier, in 2002, the Attorney General announced a nationwide sweep of identity theft cases involving 24 separate judicial districts. We are working with State and local law enforcement, as I mentioned earlier, in regular training conferences to engage in the technology transfer, to teach State and local law enforcement agents to investigate and prosecute identity theft cases.

The U.S. attorneys offices around the country along with the Criminal Division are working very aggressively to target identity theft cases and to aggressively prosecute those cases. We appreciate the support of law enforcement. We greatly appreciate the proposed legislation contained in H.R. 1731, which we believe is a

tailored, targeted and appropriate response to the growing problem of identity fraud.

We believe that the President's budget, the Administration's budget, contains sufficient resources to support the Department's effort against identity fraud and to support all the efforts in our work with State and local law enforcement, the U.S. attorneys offices, the Criminal Division and working with regulatory agencies like the FTC, the law enforcement agencies like the Secret Service. We greatly appreciate the Subcommittee's support of these efforts.

Mr. COBLE. What was the President's request in his budget for this?

Mr. COLEMAN. Mr. Chairman, I don't know that is there a specific figure in the President's budget that is earmarked or somehow identified to identity theft.

Mr. COBLE. Mr. Johnson, after having reviewed the two bills before us, would you offer changes, additions or removals, from either of the two bills that would make them more appropriate in your mind?

Mr. JOHNSON. Mr. Chairman, not at this time would we recommend any changes. The Secret Service believes that the legislation has merit as an individual tool that law enforcement can use to protect critical infrastructure and financial infrastructures.

Mr. COBLE. Mr. Ryan, in your testimony, you advocate the development of national standards for the protection of personal information. Elaborate on this suggestion and what type of standards would you suggest.

Mr. RYAN. Mr. Chairman, for example, there are—there are several active public policy issues that are either before Congress or will come before Congress. One example, perhaps, would be in the protection of Social Security numbers. There are various bills that would ban the public display and availability of Social Security numbers. Obviously, we support that.

But that would also restrict the use and the ability to gather Social Security numbers that can be important for credit grantors and financial institutions. So if and when Congress takes up a set of restrictions on the use and publication and openness of Social Security numbers, it makes a lot of sense from our perspective that would set a national standard so we don't have different rules among the States.

Mr. COBLE. Mr. Cannon, as with many criminal investigations, sharing information within the law enforcement community is crucial. With regard to identity theft cases, what partnerships have local departments formed with Federal law enforcement agencies to address the problem?

Mr. CANNON. There are a number of multi-jurisdictional task forces. I must credit the Secret Service also, in fact, for the training they provide to the local jurisdictions in being able to know what to look for and, once they know what to look for, then where to go with it. So that is a key component.

Mr. COBLE. I thank you. I recognize the gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman.

And I want to thank Mr. Cannon for his willingness to come at the late hour. We had another witness scheduled who, unfortunately, had to cancel, and we appreciate you filling in.

You mentioned the case where someone had lived in one State, lost credit information in another; the credit information was used in a third. You represent mostly local and State officials and some Federal.

Mr. CANNON. I represent everybody. If they wear a badge, I am representing them.

Mr. SCOTT. Most would be local and State.

Mr. CANNON. I represent quite a few of those. I do have a significant amount of Federal law enforcement officers in my organization here in D.C.; and having served on both sides, I feel both pains.

Mr. SCOTT. Let me ask you, if someone were to be the victim in that situation, who would they call?

Mr. CANNON. They are going to pick the phone up and call 911 and get the local officer to come out, whether it be the municipal police officer, the county sheriff or the township officer. And that is one of the key things—that individual has to have a central place to go. And the training that is needed—Secret Service provides great training in regards to that. I was pleased to hear something in regard to a central clearinghouse.

Secret Service does—and I am sure Mr. Johnson is going to love me putting work on him—the Secret Service does have a tremendous resource available to serve as a focal point for the collection of certain data that, once that data is then collected, it can then be used, similar to the NCIC system that is currently in place by the FBI.

The people involved in identity theft, they don't do it once. They are involved in multiple identity thefts spanning the Nation. As a matter of fact, I don't know whether I can say luckily, but fortunately, I just finished working an identity theft case for the U.S. Mint where an employee had stolen someone else's credit card and then used that it. And the actual victim in this one was the Federal Government—by stealing this individual's Government credit card. And he didn't stay in D.C.; he went around doing this.

One of the problems is, once we get this investigation underway and we identify the different jurisdictions, there is no coordinated prosecution effort that we could use at that point. We were able to prosecute him in multiple States, but then you get the problem of who comes first, who is going to get him, where is he going to serve the time?

Mr. SCOTT. There is enough of a paper trail out there that if somebody investigated it, you could solve the crime?

Mr. CANNON. Absolutely.

Mr. SCOTT. In a normal case where you call the credit card company—when you find out there are some bogus charges, you call your credit card company, they cancel the card, does anybody ever at that point—and cancel the charges, so that the card holder isn't at a loss—how many people—do the people call the police?

Mr. CANNON. The first call isn't to the credit card company. A lot of times it is the credit card company telling you that your identity has been stolen. And then at that point, a lot of times the police or law enforcement is never notified of that. That is also a problem, because if you don't know what is going on, then you can't combat it.

If you have a group working a specific area that could be isolated and the Secret Service could identify, they need to be on top of it as quickly as possible. But the failure to notify, that creates a whole separate problem there.

Mr. SCOTT. Mr. Ryan, if people actually did notify—I mean you have access to all the problems that occur. What would happen if people notified the police? Do they have enough resources to actually follow through on all of these cases?

Mr. RYAN. Congressman Scott, I can't really speak. My sense is that law enforcement does need more resources at all levels, local, State and Federal. That would be speaking as a layman. Our company works closely with law enforcement. But more resources are important from our perspective.

Mr. SCOTT. How often does your agency report run of the mill credit card fraud to the police? Is that a routine referral—every time you get somebody with a stolen credit card, you routinely report it to the police?

Mr. RYAN. What is more routine, Congressman, is when we have evidence of rings—keep in mind that there are two broad forms, I would say, of identity fraud. There is still—although rings are a very important and growing most sinister part of it, there is also a good deal of identity fraud that is a crime of opportunity by family members.

And so our management of our fraud victim unit will pick up the phone and call their appropriate law enforcement. We have excellent relations with the Secret Service, FBI, with local law enforcement agencies, financial crime units, et cetera. Our folks will pick up the phone and call appropriate law enforcement when we uncover or we know about a ring. We know that they will want to know about it.

Mr. COBLE. The gentleman from California, Mr. Schiff.

Mr. SCHIFF. Thank you, Mr. Chairman.

I want to begin by thanking my colleague, Mr. Carter, for his initiative on this issue.

It has been a pleasure working with you and your staff.

The bill was originally introduced in the Senate, Senator Feinstein and Senator Kyl having worked with the Justice Department. Did you work with them on the drafting at that time?

Mr. COLEMAN. I did not. I was still in the Southern District of New York as a line prosecutor at that time.

Mr. SCHIFF. Couple of questions about some of the language in the bill, trying to get a sense of the scope of the language. In section A where the offenses are defined, it refers to a means of identification of another person. I take it by the choice of that language that these enhancements apply when the fraudulent identification is that of another existing person, either live or deceased, but an actual individual, so in the case of a garden-variety immigration case where somebody fabricates an identity card out of whole cloth, not referring to any other person but merely invents a persona, that that would not be included within the sweep of this.

[11 a.m.]

Mr. COLEMAN. I believe that is correct. That is my understanding of how the legislation was drafted in my construction of the plain language. Presumably a court could take a different view in a par-

ticular case, but I believe it is fair to say that, on the face of it, the plain language would exclude cases of a fictitious identity as opposed to the theft of an existing identity.

Mr. SCHIFF. I think that is significant. I think that is correct looking at section 1028, which is also distinguished in its use of language between the possession of a false identification document and a means of identification of another person. But the reason I think it is significant is that otherwise you would potentially have an enhancement for everyone who illegally enters the country, that they would be committing one crime entering the country and they would be committing a second crime having a false document, but there wouldn't be another victim in the sense that no one's identity had been stolen to facilitate that crime.

The other question I wanted to ask refers to the changes that are made to section 1028 (a)(3) in section 3 of the bill,

and that is a—what the bill changes is subsection 7—(a)(7)—which provides for currently the transfer or use without lawful authority of the means of identification of another person. This would add possession to that.

I guess my question is, much of subsection (7) overlaps with subsections (1), (2) and (3) in the sense that subsection (a)(1) says if you knowingly produce a document, subsection (2) is if you knowingly transfer a document, and subsection (3) is if you knowingly possession five of these. What do you add with subsection (7) other than the fact that you don't need five of these anymore that is not already covered in (1), (2) and (3)?

Mr. COLEMAN. Well, I believe the one that jumps out at me is the possession prong, so that it is no longer required to show a transfer, necessarily. The prosecutor can simply prove that the defendant possessed a stolen identity in order to satisfy the requirements of 1028(a)(7).

Mr. SCHIFF. In 1028(a)(3) possession is also all that is required. You are required to possess five of these. I guess my question was, if we reduce five to one, would that accomplish the same goal?

Mr. COLEMAN. It may do that. I would have to look at it a little more closely and consult with my colleagues, but I believe that may satisfy that same goal.

Mr. SCHIFF. Do you know whether in the sentencing guidelines the guidelines distinguish between the recommended sentence or the range for the use of a fraudulent ID that is not based on a real person and the use of a fraudulent ID that has been appropriated from a real person?

Mr. COLEMAN. I believe that the current state of the guidelines are more restrictive in that they require proof of such facts as producing multiple identity documents with an access device that creates identification cards or identification devices. I don't believe that there is any enhancement for the mere possession of a stolen identity. So this would——

Mr. SCHIFF. I understand that. But my question is, under existing law or under this new statute there are two kinds of identity crimes: One is where you create a false ID which is prohibited by 1028; the other is where you basically appropriate the ID of another person. In the one case, you have committed a crime, but there is no individual other victim out there, the society as a whole

is a victim. In the second case, you have the society as a whole as a victim, but somebody's identity has been stolen and has therefore suffered the loss of the identity and having to go through all the trouble of correcting that.

I was wondering if the sentencing guidelines currently distinguish between the two of the greater recommended sentences for where you appropriate someone's ID and where you fabricate one out of whole cloth.

Mr. COLEMAN. I don't believe they do. I don't believe the guidelines recognize the increased damage that is caused by hijacking the identity of an existing individual as opposed to just creating a fictitious identity. That is one of the benefits that the Department sees in the proposed legislation.

Mr. SCHIFF. Thank you, Mr. Chairman.

Mr. COBLE. The gentleman's time has expired.

Even though Mr. Carter does not sit as a Member of the Subcommittee, he is a sponsor of one of the two bills before us. I will recognize him without objection for 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman. Thank you, Ranking Member.

I want to ask you a couple of questions. In his testimony—this is to Mr. Coleman. In his testimony in a joint hearing last year for this Subcommittee and the Subcommittee on Immigration, Border Security, and Claims on identity theft and identity fraud, U.S. Attorney Paul McNulty testified I think that probably the most significant weakness has been identified by the Attorney General in the proposal to increase the penalties for general false identity statute which is 18 USC 1028. The problem with the statute is that the penalties essentially don't have any effect whatsoever. They are essentially lumped in with the underlying fraud that is occurring. So there is no incentive whatsoever to prosecute someone for identity card possession in combination with the false form that has been filled out.

H.R. 1731 has been drafted in response to this concern. Would you mind elaborating on what those weaknesses are and discuss how H.R. 1731 will address them?

Mr. COLEMAN. I would be happy to do that. Let me start, Representative Carter, by saying how grateful the Department of Justice is for your sponsorship of this legislation and your commitment to addressing this important problem, as we are grateful to Mr. Schiff's cosponsorship of the bill.

With the existing penalties for identity theft, a prosecutor like myself will ordinarily charge some other crime that has a higher penalty. For example, if the defendant committed mail fraud or wire fraud and also committed identity theft as defined by section 1028(a)(7), the usual practice is simply to charge the most serious readily provable offense, which is usually something else.

There are rare cases—and I say rare based on several years of experience handling all types of fraud cases, that the case is rather rare where identity theft as currently defined under section 1028(a)(7) is the most serious readily provable offense. So adding an identity theft charge under existing law does two things: It makes the case harder to prove and harder to charge, but it does not increase the potential sentence. So for a prosecutor there is

very little incentive to charge identity theft under existing law, and there is very little incentive for criminals to alter their conduct by avoiding committing identity theft. If they are going to commit a crime anyway, they don't get any worse punishment by adding identity theft to it.

H.R. 1731 is targeted at exactly that problem that U.S. Attorney McNulty articulated so eloquently in his previous testimony, and we believe that H.R. 1731 would result in much more frequent charging of identity theft and send a message that this is a serious crime that is being addressed seriously.

Mr. CARTER. Thank you.

I will address this to everybody out there. The Social Security Administration Office of the Inspector General has suggested to this Committee that two felony violations not currently listed in 18 USC 1028(a)(3) that could involve the transfer, possession, and use without lawful authority of any other personal means of identification, that this should be added to this bill. These are 18 USC 371 relating to conspiracy to commit offense against or defraud the United States, and 18 USC 641 relating to the theft of public money, property, or records.

Given the dramatic increase of identity theft actions against the Federal benefits programs such as Social Security benefits, veterans benefits, workmen's compensation benefits, Medicare fraud, shouldn't 18 USC 371 be included in this bill? Does anybody want to address that?

Mr. COLEMAN. Representative Carter, the Department has not taken a formal position on that proposal, but we are a little bit concerned about the inclusion of section 371. It does give some pause to consider including that particular provision, which Mr. Schiff and other prosecutors know is often referred to as "the prosecutor's darling." I would say the vast majority of Federal criminal cases include a conspiracy charge, and that really changes the tenor of the legislation. It would change the tenor of the legislation from a narrowly focused and targeted enhancement to the existing identity theft law to a much broader change in the Criminal Code.

Mr. CARTER. One more question. Somebody might know the answer to this.

The other day I was happening to dig through some old papers. I found an original Social Security card for my father, and printed at the bottom of the card it said "Not For Identification Purposes." what happened? Does anybody have any idea why all of a sudden our grades are posted in college by Social Security numbers and so many other things are done as identifier when it was clearly designated in the original Social Security it was not for identification purposes? Anybody know the answer?

Mr. RYAN. I will step forward, Congressman. Because it possessed the virtue of being a unique identifier that bridges all systems, all other infrastructure. So over time it came to be exploited.

Mr. CARTER. It is also becoming a unique door-opener to get into some of this stuff.

Mr. SCHIFF. Would the gentleman yield for a moment?

Mr. CARTER. Yes, sir.

Mr. SCHIFF. It is an interesting question, if this is your father's identification.

Mr. CARTER. Yes. It was probably an original.

Mr. SCHIFF. If someone stole your father's Social Security card and used it, there would probably be a problem of proof because it says on it Not For Identification Purposes. So would it be an identification document under the section if the card itself says not for identification purposes?

Mr. CARTER. It probably would not. I agree. But it is interesting that it has changed so much in the history of this country.

Mr. COBLE. The gentleman's time has expired.

Folks, I think we have time for a second round. Let me start a second round here.

Mr. Coleman, I am told that many criminals purchase a document or breeder document which enables them to obtain legitimate Social Security numbers and other genuine documents. What can be done to combat this growing problem?

Mr. COLEMAN. Mr. Chairman, this is exactly the type of case that we believe H.R. 1731 would help to remedy. In many of these cases identity theft offense is a derivative offense. There is some other Federal crime that is being committed, whether it is mail fraud, wire fraud, embezzlement or some other baseline offense. Identity theft goes on top of that and makes it worse; and in some of these breeder cases H.R. 1731 would define that kind of conduct as more serious conduct, as aggravated identity theft and impose enhanced penalties for that type of conduct. It would also streamline the proof process so that prosecutors would not be constrained by State law requirements in order to effectively prosecute these cases. So we believe that that is a good illustration of why this legislation would help to address the problem.

Mr. COBLE. Mr. Johnson, insider threat whereby employees have access to information that they subsequently use to their own benefit to the detriment of innocent third parties, what steps do you think the Congress can take to address these insider threat activities and what can employers do to prevent such threats that they may not be doing now?

Mr. JOHNSON. Currently, the Secret Service, in conjunction with CERT and Carnegie Melon University, are conducting an inside threat study due for release in the coming months. That would help private industry, businesses, help them identify the insider threat that they may have in their company. What we have seen with companies in insider threats or what we suggest to those companies are, when the employee leaves the company, is to erase their access or deny their access to the systems that they once were privy to. Also to change the fire wall, change passwords.

You can go to different—a lot of companies will not do that initially, and often it comes back to be—if an intrusion or the system is taken down, it is a lot easier for the Secret Service to investigate an insider threat as opposed to a hacking situation that may come from another country. It makes it much more difficult. So, basically, Mr. Chairman, it is a common sense issue to dealing with your employee.

Mr. COBLE. Thank you, Mr. Johnson.

Mr. Ryan, I read a recent article in North Carolina about an employment agency that went out of business; and they left all the job applications along with photocopies of drivers licenses, Social Secu-

rity numbers, et cetera, in a box on the curb to be collected as garbage. What can be done to address the issue of third party handling of personnel—personal information such as I just outlined?

Mr. RYAN. Mr. Chairman, I feel more comfortable speaking within the framework of financial institutions and consumer credit reporting agencies. Within that universe we are covered by the information safeguarding rules of Gramm-Leach-Bliley, Fair Credit Reporting Act that has certain provisions dealing with the safeguarding of disposed information. I am a little out of my realm in dealing with a firm that is not governed under financial institutions or credit reporting law.

Mr. COBLE. Do any of the other witnesses feel comfortable putting your oars into those waters? The situation seems to me invites problems when you abandon property like that and just leave it to the public at large.

In any event, thank you, gentlemen.

I recognize the gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Coleman, when you use the term "identity theft," what portion of those kinds of cases are consumer identity theft as opposed to immigration or other kinds of identity theft?

Mr. COLEMAN. Representative Scott, I don't have the numbers. I don't have the breakdown by consumer cases as opposed to immigration or other offenses, so I wouldn't even want to hazard a guess.

Mr. SCOTT. It has been estimated that over nine million people last year were victims of identify theft. How many of those cases were investigated as crimes?

Mr. COLEMAN. Again, I don't have the figures, but one would have to total up all of the Federal cases that were investigated either as identity theft cases and charged as identity theft cases or charged as something else, which is usually more common, theft or fraud or any number of other crimes. Then you would have to add on top of that State crimes, local law enforcement matters, matters that were not charged. So it would be a hard task to get that figure, I believe.

Mr. SCOTT. If we just looked at the kind of credit theft where you use somebody's credit, either credit card or get a mortgage in somebody else's name and run away with the money, doesn't matter what you charge it as—I mean, it is nice to call it identity theft but, if you catch the guy and send him to jail, it doesn't matter what you are convicted of. It doesn't seem to me that it is important what code section you got them under. You caught them and you sent them to jail.

How many people would be subject to prosecution under H.R. 1731 that are not subject to prosecution?

Mr. COLEMAN. It is hard to put an exact figure on it, but we believe that the number of identity theft prosecutions would increase substantially.

Mr. SCOTT. How many prosecutions would go up? I mean, is there anybody out there that is committing a crime that would be subject to prosecution under H.R. 1731 that is not already subject to prosecution?

Mr. COLEMAN. Certainly there was a gap in existing law which covered international terrorism cases but not domestic terrorism cases. So that the proposed legislation H.R. 1731 fills in a gap in those types of cases by creating a 5-year enhanced penalty for identity used in the service of terrorism.

Mr. SCOTT. But you could have convicted the person of terrorism anyway.

Mr. COLEMAN. Well, when you say we could have convicted the person of terrorism, there are often difficulties in the proof. There are often difficulties in finding an appropriate charge and proving an appropriate charge.

One of the great benefits of the proposed legislation is it defines a category of aggravated identity theft, and it streamlines and simplifies the proof process so that we, as prosecutors, are not constrained by, for example, State law, mental State requirements that often create problems with prosecuting these cases.

Mr. SCOTT. Do you have many people who are being charged for subsequent offenses, that is to say, that the penalty for the first offense didn't deter them from doing it again?

Mr. COLEMAN. Again, I don't have figures on that. Certainly there would be increased penalties simply based on the criminal history provisions of the sentencing guidelines for recidivist offenders. But given many of the cases that we have seen of identity fraud result in sentences that do not adequately reflect the seriousness of the conduct, we believe that there is great need for additional deterrence and that this legislation improves that.

Mr. SCOTT. But you are not aware of anybody who—many people that have been convicted of second offenses.

Mr. COLEMAN. Again, Representative Scott, I don't have the figures; and I wouldn't want to guess.

Mr. SCOTT. How often does the Department of Justice prosecute cases where the loss is under a couple of thousand dollars?

Mr. COLEMAN. There are substantial number of those cases. Again, I don't have statistics that I could cite to you, but certainly in my own experience as a prosecutor I have handled small cases. There is a famous Supreme Court case, whose name I can't remember sitting here, which says that there is a long history in this country of deciding important issues on cases that involve no more than a few dollars.

So there are resource constraints that cause U.S. Attorneys Offices, for example, to turn away cases that are not above a certain limit, but there are exceptions to that that allow us to bring smaller cases.

Mr. SCOTT. That is fine. One of the bills before us will address that resource problem. Thank you.

Mr. COBLE. I thank the gentleman.

The gentleman from California.

Mr. SCHIFF. Mr. Chairman, I wanted to follow up on the issue that I discussed a little earlier and that is the language and means of identification of another person. In the first section that provides the 2-year enhancement it makes reference to means of identification of another person, which I think is an appropriate narrowing of the statute so that it doesn't reach everyone who commits an immigration violation which, like incorporating 371, would expand

the scope of this very significantly. It also recognizes that there is no second victim in the case of someone who merely uses a false document not attached to another real person.

But I wonder whether the same logic applies to the terrorism enhancement. The gravamen of the terrorism offense is so significant in most of the sections that the threat of the consecutive sentence for the false ID is a relatively minor factor. When you look at some of the sections in 2332 that apply to acts of terrorism, transcending national boundaries, relating to biological weapons, relating to chemical weapons, relating to kidnap or killings of congressional, Cabinet, or Supreme Court members, nuclear materials, plastic explosives, probably the last thing to be concerned about by potential terrorist is an enhancement for having a false ID.

But there are a few sections in here such as those relating to providing material support for terrorists, relating to providing material store for terrorist organizations, relating to financing of terrorism, where the section may be more significant.

I wonder, because the range of offenses is so narrow here and you don't have the same concern that you would in the first section, whether it would make sense to include not only when you use the means of identification of another person but when you use a false or fraudulent identification document, whether or not it pertains to another person.

If a member of al-Qaeda or someone supporting al-Qaeda with a financial support is using false identification to do so, we probably don't need to be as concerned about the fact there is no additional individual victim whose identity is stolen but the fact that they are using this technique that gives prosecutors another tool to go after them.

So we may want to think about whether it makes sense that—given the scope of the list of offenses is so narrow in part 2 and whether the scope of the documents that are used can be broader.

Mr. COLEMAN. We would certainly be happy to work with the Subcommittee to try to refine some of those definitions and work on the drafting to see if there were a way to address those concerns either in this legislation or perhaps in a separate piece of legislation.

Mr. SCHIFF. For example, if someone uses a false document to come into the country to hijack a plane to crash into a building, the fact that that false identification document isn't connected with a real person is of very little significance. If you arrest them before they commit the act and you can prove that it was in connection with a conspiracy to commit the act, you would certainly, I think, want the ability to make use of this section.

I yield back.

Mr. COBLE. I thank the gentleman.

The gentleman from Texas is recognized for 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman. I would like to thank you, Mr. Chairman, and your staff for holding this hearing. I would like to thank Congressman Schiff for joining me in support of this legislation.

Gentlemen, I have one simple question. Is there anything—and I—first let me say that what Congressman Schiff was talking about makes good sense to me and maybe that is something we need to

look at. Is there anything that you can think of that will make this a better piece of legislation that we should consider at this time? And I will lay that out for any of you and all of you. Does anyone have any suggestions of anything we could add that would improve this?

Mr. COLEMAN. Representative Carter, sitting here today, the Department doesn't have any suggestions for additional matters, but we would certainly be happy to work with the Committee to examine other possibilities.

Again, we greatly appreciate your support on this issue.

Mr. CARTER. Thank you, Mr. Chairman. I yield back my time.

Mr. COBLE. I thank the gentleman.

Gentlemen, again we thank you.

Mr. SCOTT. I would ask unanimous consent that the record include a copy of the speech given by Supreme Court Justice Kennedy on August 14, 2003, in which he discusses mandatory minimums.

Mr. COBLE. Without objection, it will be received in the record.

[The speech given by Supreme Court Justice Kennedy can be found in the Appendix.]

Mr. COBLE. I thank you all for your testimony. The Subcommittee very much appreciates your contribution and those in the audience as well.

This concludes the legislative hearing on H.R. 1731, the "Identity Theft Penalty Enhancement Act," and H.R. 3693, the "Identity Theft Investigation and Prosecution Act of 2003." The record will remain open for oneweek. Thank you for your cooperation.

The Subcommittee stands adjourned.

[Whereupon, at 11:30 a.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF LOUIS P. CANNON

Good morning, Mr. Chairman, Ranking Member Scott and distinguished members of the House Subcommittee on Crime, Terrorism and Homeland Security. My name is Lou Cannon, and I am a 22-year veteran of the Washington, D.C. Metropolitan Police Department and currently serve as an Inspector with United States Mint Police. I am also the elected President of District of Columbia Lodge #1, which represents more than 9,500 law enforcement officers throughout the greater Washington, D.C. metropolitan area. Nationally, the F.O.P. is the nation's largest law enforcement labor organization, representing more than 311,000 rank-and-file law enforcement officers in every region of the country.

I am here this morning at the request of Chuck Canterbury, National President of the F.O.P. to discuss two pieces of legislation, H.R. 1731, the "Identity Theft Penalty Enhancement Act of 2004" and H.R. 3693, the "Identity Theft Investigation and Prosecution Act" and also to give this Subcommittee the views of the Fraternal Order of Police on the rise of identity crimes in the United States.

The technology of the information age has allowed criminals to commit "traditional" crimes in new ways. Identity theft is one such example. A criminal who obtains key pieces of personal information—Social Security and driver's license numbers, for example—can then commit fraud and other crimes by purchasing credit, merchandise and services in the name of the victim.

Identity theft is the fastest growing crime in the United States. The Federal Trade Commission (FTC) found that complaints of identity theft increased eighty-seven percent (87%) between 2001 and 2002, and more than 161,000 complaints were received by the agency last year.

The cost of these crimes is high. The FTC estimates that the loss to the businesses and financial institutions to be approximately $47.6 billion, and the cost to individual consumers is estimated to be approximately $5 billion.

The F.O.P. was very pleased to have played a leadership role in the recent enactment of S. 1581, the "Identify Theft Victims Assistance Act," which was passed as a component of H.R. 2622, the "Fair and Accurate Credit Transactions Act" and signed into law in December of last year. This legislation gives law enforcement officers the tools to better investigate identity theft crimes by allowing victims to designate local law enforcement as their agent in obtaining business records—applications for credit, records of sales, and other documents—related to ongoing fraud. Access to such records will greatly improve the speed and effectiveness of investigations into these types of crimes. Without a court order, most creditors are unwilling to divulge information to law enforcement about open accounts because of liability concerns, and a good faith desire to protect the privacy rights of the account holder. The new law provides that a business may not be held liable for any disclosure made in good faith to further a prosecution of identity theft. This is a huge step forward for law enforcement because the lack of timely information about the fraudulent transactions delays the progress of the investigation and the chances of closing the case.

Now that Congress has addressed one of the hurdles on the ability of law enforcement to collect the information it needs to investigate such crimes, we believe that further Federal funding will enable us to aggressively investigate these cases and go after these criminals.

Legislation like H.R. 3693, offered by the Ranking Member and Chairman of this Subcommittee would authorize $100 million to the Department of Justice for the investigation and prosecution of identity theft and identity fraud cases. The legislation does not restrict how that money might be used, allowing law enforcement to de-

velop and fund its best approach, be it equipment, multijurisdictional task forces, or grants to State and local agencies.

Because the nature of these crimes make it difficult for local and State law enforcement to investigate these crimes effectively—or even take a report—the F.O.P. believes that enhanced funding will have a positive effect on the ability of law enforcement to investigate and close these types of cases. For example, a victim in South Carolina has his identity stolen while on vacation in Florida and the information is used to buy merchandise in New Jersey. Where was the crime committed—in South Carolina, where the victim resides; in Florida, where the information was stolen; or the point of purchase in New Jersey? What if the fraudulent purchase was made online? Identity theft crimes require a great deal of coordination and cooperation between law enforcement agencies. To us, it only makes sense to provide greater resources to address a type of crime that is on the rise.

Similarly, Congress should consider enhancing the available penalties to identity criminals, as is contemplated by H.R. 1731.

I want to thank Ranking Member Scott for inviting me to appear before the Subcommittee today, and I would be happy to answer any questions you might have.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

COMMITTEES:
SELECT COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEES:
INFRASTRUCTURE AND BORDER SECURITY
CYBERSECURITY, SCIENCE, AND RESEARCH & DEVELOPMENT

JUDICIARY
SUBCOMMITTEES:
CRIME
RANKING MEMBER
IMMIGRATION AND CLAIMS

SCIENCE
SUBCOMMITTEE:
SPACE AND AERONAUTICS

MEMBER
DEMOCRATIC CAUCUS POLICY AND STEERING COMMITTEE

1ST VICE CHAIR
CONGRESSIONAL BLACK CAUCUS

Congress of the United States
House of Representatives
Washington, DC 20515

WASHINGTON OFFICE
2435 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3816

DISTRICT OFFICE
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

STATEMENT BY

CONGRESSWOMAN SHEILA JACKSON LEE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY OF THE JUDICIARY COMMITTEE

H.R. 1731: THE IDENTITY THEFT PENALTY ENHANCEMENT ACT
&
H.R. 3693: IDENTITY THEFT INVESTIGATION

MARCH 23, 2004

Chairman Coble and Ranking Member Scott, thank you for holding this legislative hearing on Identity Theft. Moreover, thank you to the witness panel for taking its time to share testimony with us today. This crime is a huge concern for the United States as well as the international community because it not only allows

perpetrators to profit from a victim's personal information, but it can and has been used as an instrument to commit terrorism.

With respect to the terrorist bombings which occurred in Madrid on March 11, 2004, a form of identity fraud may have been one of the things that facilitated the attackers' success. Allegedly, the perpetrators of that horrible act detonated the explosives that were placed in a backpack by means of falsified cell phone SIM cards.

Furthermore, let us not forget, it was identity fraud that allowed the 9/11 criminals to board the aircrafts and to guide them into the Twin Towers. We definitely need legislative answers to this problem while at the same time preserving the civil rights of everyone.

H.R. 1731, Identity Theft Penalty Enhancement Act of 2004

This bill aggressively addresses our urgent need to capture many perpetrators with one initiative. However, in Section 2, it takes parole away from *all* individuals who have been charged and convicted with certain other crimes in addition to crimes associated with identity fraud.

Unfortunately, this bill may suffer from overbreadth because there is no "second chance" for charged and convicted individuals despite the fact that it does not call for a study of the recidivism rate of those charged and convicted of identity. The individual who commits the fraud along with a felony as set forth in subsection 4(c) is differentiated from the individual who commits the felony along with a crime of terrorism by the mandatory sentencing – 2 years and 5 years respectively. However, these convicted individuals are both denied parole.

H.R. 3693, Identity Theft Investigation and Prosecution Act of 2003

The legislation, H.R. 3693, that has been introduced by Mr. Scott, is a good approach to addressing the problem of identity theft. Rather than imposing sentences and a denial of parole upon all individuals who commit identity theft, it authorizes funds to be appropriated to the Department of Justice (DOJ) so that it can conduct the necessary studies on rescidivism and other relevant trends as well as decide what sentencing is appropriate for one who commits identity theft along with an underlying felony.

In Houston a few months ago, two men, Richard L. Craig, 35 and Robin L. Ross, 40 were sentenced to 8 and 5 years in prison respectively without parole for conspiracy to commit money laundering and to possess stolen mail, and with possession of stolen mail.

A Texas law makes it a felony to steal another person's identity, and then the person who commits the offense can be imprisoned and ordered to reimburse the victim for lost income or other expenses, but not for attorney's fees. This demonstrates that there are a myriad of legislative controls set to punish the identity thief. The task for us as legislators is to streamline the legislative tools that we arm our prosecutors with and design punishment very carefully after study is conducted. Mr. Scott's proposal authorizes funds to DOJ in order to initiate studies that would aid in drafting a streamlined bill to enhance penalties.

Identity theft victims now spend an average of 600 hours – often over a period of years – recovering from the crime. Being a victim costs an average of $1,400 in out-of-pocket expenses, and 185 percent increase from years before.

We must craft legislation that will not only punish the perpetrator of the identity theft but also encourage the disclosure of

information that will facilitate the re-establishment of the victim's credit-worthiness.

Thank you.

SPEECH AT THE AMERICAN BAR ASSOCIATION ANNUAL MEETING

An Address by Anthony M. Kennedy
Associate Justice, Supreme Court of the United States

August 9, 2003

© 2003 Anthony M. Kennedy
Revised August 14, 2003

Mayor Brown, President Carlton, President-elect Archer, and my fellow adherents to the Rule of Law. Thank you for your gracious welcome and for your friendship.

Since we last met in San Francisco, momentous and tragic events have occurred. Some say these events changed the world. Perhaps it is more accurate to say the world is the same, but we now have a clearer understanding of what the world is. It is a world where in every nation many people seek freedom above all, but where new enemies of freedom vow to attack it. In a sense this is nothing new. In the last century free societies were attacked from within, attacked by their own citizens, by men such as Stalin, Hitler, and Mussolini. They attacked free institutions because they did not believe an open society, committed to democracy, could provide for the security and welfare of its citizens. In this century democracy's enemies come from outside the countries they seek to destroy. They, too, see a free and open society as a threat. Once again we face an assault on freedom. Once again we can prevail.

Americans may find the new challenge surprising and disappointing. We tend to think the case has been made that a free society is a stable society, that a free society is the birthright of all people. We do not know why we must make the case all over again when judgment has been given in our favor. History, however, does not acknowledge *res judicata*. History teaches that freedom must make its case, again and again, from one generation to the next. The work of freedom is never done.

Embedded in democracy is the idea of progress. Democracy addresses injustice and corrects it. The progress is not automatic. It requires a sustained exercise of political will; and political will is shaped by rational public discourse. One of the ABA's missions is to stimulate that discourse.

The impressive, pluralistic assembly of the American Bar Association reflects many groups and interests in our society. That is fortunate, for a disproportionate share of the responsibility for moving toward progress in public affairs falls, in the

first instance at least, on those who are trained in the law. The Bar is an essential catalyst for the discourse we must commence to come closer to a more just society.

You have many issues to address. Please permit me to talk with you about two of them. The first concerns the inadequacies -- and the injustices -- in our prison and correctional systems. The second is the continuing need to teach the principles of freedom to our young people, who soon must become the principal trustees of our constitutional heritage and our most treasured institutions.

The subject of prisons and corrections may tempt some of you to tune out. You may think, "Well, I am not a criminal lawyer. The prison system is not my problem. I might tune in again when he gets to a different subject." In my submission you have the duty to stay tuned in. The subject is the concern and responsibility of every member of our profession and of every citizen. This is your justice system; these are your prisons. The Gospels' promise of mitigation at judgment if one of your fellow citizens can say, "I was in prison, and ye came unto me," does not contain an exemption for civil practitioners, or transactional lawyers, or for any other citizen. And, as I will suggest, the energies and diverse talents of the entire Bar are needed to address this matter.

Even those of us who have specific professional responsibilities for the criminal justice system can be neglectful when it comes to the subject of corrections. The focus of the legal profession, perhaps even the obsessive focus, has been on the process for determining guilt or innocence. When someone has been judged guilty and the appellate and collateral review process has ended, the legal profession seems to lose all interest. When the prisoner is taken way, our attention turns to the next case. When the door is locked against the prisoner, we do not think about what is behind it.

We have a greater responsibility. As a profession, and as a people, we should know what happens after the prisoner is taken away. To be sure the prisoner has violated the social contract; to be sure he must be punished to vindicate the law, to acknowledge the suffering of the victim, and to deter future crimes. Still, the prisoner is a person; still, he or she is part of the family of humankind.

Were we to enter the hidden world of punishment, we should be startled by what we see. Consider its remarkable scale. The nationwide inmate population today is about 2.1 million people. In California, even as we meet, this State alone keeps over 160,000 persons behind bars. In countries such as England,

Italy, France and Germany, the incarceration rate is about 1 in 1,000 persons. In the United States it is about 1 in 143.

We must confront another reality. Nationwide, more than 40% of the prison population consists of African-American inmates. About 10% of African-American men in their mid-to-late 20s are behind bars. In some cities more than 50% of young African-American men are under the supervision of the criminal justice system.

While economic costs, defined in simple dollar terms, are secondary to human costs, they do illustrate the scale of the criminal justice system. The cost of housing, feeding and caring for the inmate population in the United States is over 40 billion dollars per year. In the State of California alone, the cost of maintaining each inmate in the correctional system is about $26,000 per year. And despite the high expenditures in prison, there remain urgent, unmet needs in the prison system.

To compare prison costs with the cost of educating school children is, to some extent, to compare apples with oranges, because the State must assume the full burden of housing, subsistence, and medical care for prisoners. Yet the statistics are troubling. When it costs so much more to incarcerate a prisoner than to educate a child, we should take special care to ensure that we are not incarcerating too many persons for too long.

It requires one with more expertise in the area than I possess to offer a complete analysis, but it does seem justified to say this: Our resources are misspent, our punishments too severe, our sentences too long.

In the federal system the sentencing guidelines are responsible in part for the increase in prison terms. In my view the guidelines were, and are, necessary. Before they were in place, a wide disparity existed among the sentences given by different judges, and even among sentences given by a single judge. As my colleague Justice Breyer has pointed out, however, the compromise that led to the guidelines led also to an increase in the length of prison terms. We should revisit this compromise. The Federal Sentencing Guidelines should be revised downward.

By contrast to the guidelines, I can accept neither the necessity nor the wisdom of federal mandatory minimum sentences. In too many cases, mandatory minimum sentences are unwise and unjust.

Consider this case: A young man with no previous serious offense is stopped

on the George Washington Memorial Parkway near Washington D. C. by United States Park Police. He is stopped for not wearing a seatbelt. A search of the car follows and leads to the discovery of just over 5 grams of crack cocaine in the trunk. The young man is indicted in federal court. He faces a mandatory minimum sentence of five years. If he had taken an exit and left the federal road, his sentence likely would have been measured in terms of months, not years.

United States Marshals can recount the experience of leading a young man away from his family to begin serving his term. His mother says, "How long will my boy be gone?" They say "Ten years" or "15 years." Ladies and gentlemen, I submit to you that a 20-year-old does not know how long ten or fifteen years is. One day in prison is longer than almost any day you and I have had to endure. Alexander Solzhenitsyn describes just one day in prison in the literary classic "One Day in the Life of Ivan Denisovich." Ivan Denisovich had a ten-year sentence. At one point he multiplies the long days in these long years by ten. Here is his final reflection: "The end of an unclouded day. Almost a happy one. Just one of the three thousand six hundred and fifty-three days of his sentence, from bell to bell. The extra three were for leap years."

Under the federal mandatory minimum statutes a sentence can be mitigated by a prosecutorial decision not to charge certain counts. There is debate about this, but in my view a transfer of sentencing discretion from a judge to an Assistant U. S. Attorney, often not much older than the defendant, is misguided. Often these attorneys try in good faith to be fair in the exercise of discretion. The policy, nonetheless, gives the decision to an assistant prosecutor not trained in the exercise of discretion and takes discretion from the trial judge. The trial judge is the one actor in the system most experienced with exercising discretion in a transparent, open, and reasoned way. Most of the sentencing discretion should be with the judge, not the prosecutors.

Professor James Whitman considers some of these matters in his recent book *Harsh Justice*. He argues that one explanation for severe sentences is the coalescence of two views coming from different parts of the political spectrum. One view warns against being soft on crime; the other urges a rigid, egalitarian approach to sentence uniformity. Both views agree on severe sentences, and both agree on mandatory minimum sentences. Whatever the explanation, it is my hope that after those with experience and expertise in the criminal justice system study the matter, this Association will say to the

Congress of the United States: "Please do not say in cases like these the offender must serve five or ten years. Please do not use our courts but then say the judge is incapable of judging. Please, Senators and Representatives, repeal federal mandatory minimums."

The legislative branch has the obligation to determine whether a policy is wise. It is a grave mistake to retain a policy just because a court finds it constitutional. Courts may conclude the legislature is permitted to choose long sentences, but that does not mean long sentences are wise or just. Few misconceptions about government are more mischievous than the idea that a policy is sound simply because a court finds it permissible. A court decision does not excuse the political branches or the public from the responsibility for unjust laws.

To help those who are serving under the minimums, the ABA should consider a recommendation to reinvigorate the pardon process at the state and federal levels. The pardon process, of late, seems to have been drained of its moral force. Pardons have become infrequent. A people confident in its laws and institutions should not be ashamed of mercy. The greatest of poets reminds us that mercy is "mightiest in the mightiest. It becomes the throned monarch better than his crown." I hope more lawyers involved in the pardon process will say to Chief Executives, "Mr. President," or "Your Excellency, the Governor, this young man has not served his full sentence, but he has served long enough. Give him what only you can give him. Give him another chance. Give him a priceless gift. Give him liberty."

The debate over the goals of sentencing is a difficult one, but we should not cease to conduct it. Prevention and incapacitation are often legitimate goals. Some classes of criminals commit scores of offenses before they are caught, so one conviction may reflect years of criminal activity. There are realistic limits to efforts at rehabilitation. We must try, however, to bridge the gap between proper skepticism about rehabilitation on the one hand and improper refusal to acknowledge that the more than two million inmates in the United States are human beings whose minds and spirits we must try to reach. We should not ignore the efforts of the countless workers and teachers and counselors who are trying to instill some self-respect and self-reliance and self-discipline in convicted offenders. Credit must be given to the dedicated persons who conduct prison education programs. Over 90% of state prisons and 100% of federal prisons offer some kind of educational program. And about one in four state prison inmates attains a GED while in prison.

Professor Whitman concludes that the goal of the American corrections system is to degrade and demean the prisoner. That is a grave and serious charge. A purpose to degrade or demean individuals is not acceptable in a society founded on respect for the inalienable rights of the people. No public official should echo the sentiments of the Arizona sheriff who once said with great pride that he "runs a very bad jail."

It is no defense if our current prison system is more the product of neglect than of purpose. Out of sight, out of mind is an unacceptable excuse for a prison system that incarcerates over two million human beings in the United States. To that end, I hope it is not presumptuous of me to suggest that the American Bar Association should ask its President and the President-elect to instruct the appropriate committees to study these matters, and to help start a new public discussion about the prison system. It is the duty of the American people to begin that discussion at once.

In seeking to improve our corrections system, the Bar can use the full diversity of its talents. Those of you in civil practice who have expertise in coordinating groups, finding evidence, and influencing government policies have great potential to help find more just solutions and more humane policies for those who are the least deserving of our citizens, but citizens nonetheless. A decent and free society, founded in respect for the individual, ought not to run a system with a sign at the entrance for inmates saying, "Abandon Hope, All Ye Who Enter Here."

Let us turn now from the subject of those who have broken the social contract to those who soon will assume the full duty to keep it. I refer to the splendid young people in this nation who will become the next trustees of our legal and constitutional tradition. It is my pleasure to extend formal thanks to this Association for sponsoring the program for high school students, the program called "The Dialogue on Freedom." Past-President Hirshon, President Carlton, and President-elect Archer have all devoted their personal attention to it.

This is an exercise for high school seniors or first-year college students. It could be the foundation of a full semester course, perhaps, but the exercise we suggested took one session of about 90 minutes. Our figures are imprecise, but we estimate that to date over 140,000 students have taken the class.

The students were asked to assume they were stranded in a third-world country with strong suspicions, or active hostility, to America, to its republican principles,

and to its commitment to freedom. Our objective was to show young people that our heritage can endure and spread only as a conscious act. An informed understanding of the foundations of freedom is not a genetic, inherited characteristic. It is taught. Each generation must learn and then teach it again.

I spoke with many of the instructors who presented the program. As is so often the case when we work with young people, there is good news and bad news. There is cause for concern; and there is much to inspire confidence and optimism.

The principle that often motivated the students' instinctive reaction to questions about basic principles of government was tolerance. At one level this is reassuring. Tolerance, properly understood, stems from the ideas of the Declaration of Independence and the principles embraced by the founders of the Republic. In our legal tradition, and in our constitutional heritage, tolerance follows from the premise that all persons have inalienable rights, including the right to life, liberty, and pursuit of happiness. The exercise of those rights should be respected. Hence the idea of tolerance.

The problem is that all too many young people seem to equate the idea of tolerance with the concept of relativism. This is a grave error. Unbounded relativism as a civic philosophy soon becomes passivity and indifference: No judgments can be made, for it is impossible to place one set of values over another. This is a far cry from toleration derived from a belief in universal rights. If, in the civic sphere, relativism swallows tolerance whole, belief in universal rights turns into no belief at all. According to this view, we cannot judge others because our view of rights has no greater validity than any other. Were this muddled mindset to prevail, America could not teach or transmit the principles of freedom. Some students understand this; others do not. Some teachers understand this; others do not.

Here is an example. We asked students if, when discussing political philosophy in this imaginary place, they have a civic duty to try to persuade other young people not to surrender power to an authoritarian regime. A surprising number of students believed other nations should be allowed to adopt any system and pursue any domestic policy a majority wants. We overreach, they said, if we try to influence the result by offering our views as to what is just. Then we posed a series of problems, leading to the question whether it would be wrong to intervene to prevent genocide or a holocaust. A few students persisted in saying this is not our concern. I was astounded.

This is but callous indifference masquerading as tolerance. This is the distortion of

tolerance, not fidelity to the individual dignity from which tolerance springs. By this calculus, the principles espoused by Washington, Hamilton, Madison, and Jefferson mean little.

When a few students persisted in saying those who believe in freedom should just mind their own business as to other countries, even in the case of a holocaust, the rest of the class was deeply troubled. They saw the problem. The legitimacy of a legal order based on universal values and respect for all persons at this point became more apparent. At a conceptual level, however, many had difficulty trying to escape the relativist grip.

In our profession we can appreciate that answers are not always easy when we seek to resolve concrete problems by general principles. Life generates tough cases. And tough cases require careful, mature deliberation. That is why we can make a contribution to the public discourse. Still, we must remember that the legal order rests on certain fundamental truths. These truths must be taught. We must guard against the easy slide into neglect and passivity. The Rule of Law will mean little in a society too apathetic to know that vigilance is the price of liberty.

Respect for individual dignity is a universal challenge. Trying to illustrate the point by important books the students selected was one technique used in the high school dialogues. Let me describe, though, a real instance when the choice of one book made all the difference. A few years ago, a member of the bar from California named Ed Villmoare volunteered to serve in Kosovo under the auspices of the ABA's successful CEELI program. His wife, Paula Huntley, decided to go with him and teach English to high school students in that impoverished, suffering place. She has written a fine account of the experience in a volume called *The Hemingway Book Club of Kosovo.*

She wanted to teach English but had no book. In the only store in Prishtina with any books in English she found one copy of Hemingway's *The Old Man and the Sea*. It is short, and of course is distinguished by its clear and powerful prose. She bought the book and copied it for the class. It was the only game in town. But it proved to be an excellent choice. The students in her class in Kosovo were inspired by the story of the old man, down on his luck. You will recall the story. The old man had not caught a fish for eighty-four days, and the townspeople thought he was finished. Then, when he hooked a huge fish, he had to battle forces far greater than he. The young people in a war-torn nation related to that. They understood, too, what it means to encounter defeat but remain unbroken and dignified by the struggle.

The children in Kosovo understood that liberty means the right to search for dignity. So they respected the old man's struggle. By their ready acceptance of these universal ideas they taught their teacher, and they teach us, that individuals must always be willing to contend against greater forces to build a better world. Thus, the formal principles of freedom must be taught to preserve our heritage; but we will find that the desire for freedom is the birthright and the natural aspiration of all decent people.

Our own legal tradition has been shaped by persons who know there is injustice but must resort to the law to establish the general principles for righting it. Over 115 years ago, in this city, a man called Yick Wo went to court when local officials denied him a permit for his laundry business. He came to the Supreme Court of the United States. His case generated one of the most important equal protection decisions ever written. It is a tribute to our law and to our profession that a case involving a foreign national gave meaning and scope to the equal protection rights of all Americans. Our case law system is built on the idea that individuals in any era can strive to vindicate personal rights, and that by their effort our law emerges stronger than before.

In this process, lawyers know that every battle does not bring victory. There will be defeats, but the defeats will not break our will. In day-to-day debates on how to relate the law to our civic discourse and our lasting traditions, we must insist on rational, principled judgment. By doing so we advance the mission of a free people.

I hope that during this time in San Francisco you will find new ideas, new insights, and new inspiration for your work. Jefferson talked often of freedom and self-government. One cannot exist without the other. It is the mission of our profession to help preserve the role of this nation as the guardian of what Jefferson called the sacred fire of freedom and self-government, keeping it in trust for those other nations benign and enlightened enough to seek it for themselves. Thank you for being united in this historic cause.

○