CYBER-SECURITY ENHANCEMENT AND CONSUMER DATA PROTECTION ACT OF 2006

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

ON

H.R. 5318

MAY 11, 2006

Serial No. 109–106

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PRINTING OFFICE
27–475 PDF WASHINGTON : 2006

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

COMMITTEE ON 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
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

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
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
CHRIS VAN HOLLEN, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida

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

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

DANIEL E. LUNGREN, California
MARK GREEN, Wisconsin
TOM FEENEY, Florida
STEVE CHABOT, Ohio
RIC KELLER, Florida
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
LOUIE GOHMERT, Texas

ROBERT C. SCOTT, Virginia
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

MICHAEL VOLKOV, *Chief Counsel*
DAVID BRINK, *Counsel*
CAROLINE LYNCH, *Counsel*
JASON CERVENAK, *Full Committee Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MAY 11, 2006

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

WITNESSES

Ms. Laura H. Parsky, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice	
Oral Testimony	5
Prepared Statement	8
Mr. Joseph LaRocca, Vice President, Loss Prevention, National Retail Federation	
Oral Testimony	26
Prepared Statement	27
Ms. Anne Wallace, Executive Director, Identity Theft Assistance Corporation	
Oral Testimony	29
Prepared Statement	32
Ms. Susanna Montezemolo, Policy Analyst, Consumers Union	
Oral Testimony	39
Prepared Statement	40

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Business Software Alliance	60

CYBER-SECURITY ENHANCEMENT AND CONSUMER DATA PROTECTION ACT OF 2006

THURSDAY, MAY 11, 2006

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

The Subcommittee met, pursuant to notice, at 9:02 a.m., in Room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chairman of the Subcommittee) presiding.

Mr. COBLE. Good morning, ladies and gentlemen.

We welcome you to this important hearing on our Nation's computer crime laws.

Today, the Subcommittee will be conducting a legislative hearing on H.R. 5318, the "Cyber-Security Enforcement and Consumer Data Protection Act of 2006," which was introduced by Chairman Sensenbrenner, Mr. Smith of Texas, Mr. Feeney of Florida, Mr. Schiff of California, and Ms. Pryce of Ohio, and I.

The Internet revolutionized our society in many ways. While its benefits abound and extend from our largest corporations to remote rural areas, nefarious tech-savvy individuals in the United States and abroad have, unfortunately, been able to exploit the Internet for criminal means.

Cyber-crime is often faceless and has proven to defy traditional investigative and prosecutorial tools. As a result, the scope and frequency of cyber-crime is growing rapidly and now includes many intentional criminal syndicates and is threatening our economy, safety, and prosperity.

Any legislation to enhance cyber-security should begin, it appears to me, with three core principles. First, it should create a strong deterrent to prevent past crimes from being repeated and prevent future attempts to develop new criminal techniques that could be used to exploit the Internet and its users. The one thing we know about Internet fraudsters is that they are a sophisticated and intelligent group of criminals.

Secondly, it must protect consumers' personally identifiable data, which, in one way or another, is the ultimate target of all cyber-criminals.

Finally, we must provide the Department of Justice and private sector with the necessary resources to investigate and prosecute cyber-criminals.

H.R. 5318 purports to address these principles by expanding the definition of "protected computer" to ensure that the criminal—that

the Federal criminal law protects personal data found in a broader range of databases and systems. It addresses the growing use of botnets to commit computer crimes by prohibiting both the threat and the use of botnets to unlawfully access a computer and also creates the prohibition against unlawfully obtaining certain information that can be used as a means of identification.

H.R. 5318 also addresses these principles by adding section 1030 to the Racketeer Influence and Corrupt Organization, the RICO statute, which provides the Department of Justice with a much-needed tool to investigate and prosecute organized crime syndicates, which increasingly use sophisticated cyber-schemes to commit criminal acts.

The bill also increases the maximum punishment for violating section 1030 to 30 years and requires a defendant to forfeit any real or personal property that was used to commit or is a form of a cyber-crime.

I look forward to learning more about this bill and thank all of our witnesses for participating in today's hearing.

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

Mr. SCOTT. Thank you, Mr. Chairman.

And I won't ask you to describe those technical terms that you mentioned in your statement.

Mr. COBLE. I refuse to respond to that. But good try, Bobby. [Laughter.]

Mr. SCOTT. Thank you, Mr. Chairman, for holding the hearing on 15—5318, the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006."

While some tweaking of the bill is, I think, desirable to clarify the intent and application of some of its provisions, in general it does contain reasonable provisions aimed at better addressing the growing problem of computer-based crimes, including the problems associated with security breaches of personal individual data systems, such as the well-publicized breach involving ChoicePoint Corporation.

However, the bill touches on only a part of the needed solutions in the issue of security breach and risk of identity theft and other improper uses of personal individual data.

Other important components of an effective response to the problem include requiring an effective safeguard for the protection of personal individual data, notification of individuals when their personal data is exposed through breach, allowing individuals to control access to or sharing of their personal data with others through a security freeze or similar mechanisms, and allowing individuals access to their own data to check it for inaccuracies and to correct any inaccuracies found.

Other bills before Congress in other Committees address some of these issues, some better than others. So, Mr. Chairman, I hope that we can work together to ensure that if this bill becomes a part of a larger legislative scheme to address security breaches, that the other parts of the scheme actually enhance individual rights and protections without preempting the States' ability to continue to do so effectively as well.

While H.R. 4127 from the House Energy and Commerce Committee would do just that, I am concerned that H.R. 3997 from the Financial Services Committee might actually undermine individual rights and protections as well as preempt the States' ability to protect them.

One of the major problems stemming from security breaches is identity theft to obtain money or other valuables with someone else's personal information.

Gone are the days when computer hacking was primarily a factor of mischief or mischievous geeks or brainy youngsters just showing off what they can do with computers. Now it is primarily for crime purposes, including organized crime by Asian or East European crime syndicates.

While this bill will enhance Federal law enforcement officials' ability to redress hacking and other computer-based crimes, I remain concerned that we are still not doing what we could easily do more effectively to address issues such as identity theft.

My fear is that cases such as the case that we had—we heard in the last hearing involving Senator Domenici a few years ago, where some $800 in merchandise was charged to his stolen credit card. And we found that that crime was not being prosecuted.

The credit card companies readily absorb such losses by taking them off the victim's card, but thieves are left with the knowledge that if they don't steal too much, they can do so with impunity. I believe that a dedicated FBI and assisting U.S. attorneys' operation whose only job is to go after identity thieves, working in partnership with State law enforcement, would quickly reverse the expectation that thieves have on this front.

Now, Mr. Chairman, you and I, along with a number of other cosponsors, filed a bill last year to authorize $100 million for such a unit. The bill did not pass, but we were successful in getting $10 million authorized in the ID Theft Penalty Enhancement Act. And I'd be curious to learn from the Department of Justice how that authorization is being utilized.

I'm aware that the number of ID theft victims in the country have begun to go down, while the number of total losses from ID theft has continued to rise. Privacy Rights Clearing House recently reported that the number of U.S. adult victims of identity theft decreased from 10 million in calendar year 2002 down to 8.9 million in 2005. Whereas the total amount of the theft rose from $53 billion in 2003 to $56 billion in 2005, with the mean amount per victim actually rising from a little over $5,200 to $6,300.

So, Mr. Chairman, I'd like to continue to see decreases in the number of ID theft victims as well as seeing the amounts of the thefts involved also decrease. If DOJ has not established a dedicated ID theft investigation and prosecution unit, as we thought we would need, I suspect that that would be the missing link and hope that we can work together to ensure that that happens.

I look forward to the testimony of our witnesses and working with you, Mr. Chairman, to further the protections for individuals and companies against computer-based crimes.

Mr. COBLE. I thank you, Mr. Scott.

Ladies and gentlemen, it's the practice of the Subcommittee to swear in all witnesses appearing before it. So if you would please stand and raise your right hands?

[Witnesses sworn.]

Mr. COBLE. Let the record show that each of the witnesses answered in the affirmative. You may be seated.

We are pleased to have four distinguished witnesses with us today. Our first witness is Deputy Assistant Attorney General Laura Parsky. Ms. Parsky was appointed as deputy assistant attorney general in the Criminal Division in April 2004 and is responsible for overseeing the Computer Crime and Intellectual Property Section.

She initially joined the department through the honors program as a trial attorney in the Criminal Division's Narcotics and Dangerous Drugs Section. Ms. Parsky graduated magna cum laude from Yale University and obtained her law degree from the Boalt Hall School of Law at the University of California at Berkeley.

Our second witness is Mr. Joseph LaRocca, vice president of loss prevention with the National Retail Federation. Mr. LaRocca has over 19 years of retail loss prevention, security, and operations experience. In January 2005, he joined the National Retail Federation as vice president of loss prevention.

Mr. LaRocca has presented to thousands of loss prevention, law enforcement, and retail executives in North America on issues ranging from organized retail crime to loss prevention best practices. His content has appeared on CNN, Fox News, the Today Show, and has been published in *Time, Consumer Reports, the Wall Street Journal, New York Times,* and a host of other trade, local, and national publications.

Our third witness is Ms. Anne Wallace. Ms. Wallace is the executive director of the Identity Theft Assistance Corporation, a not-for-profit corporation that operates the Identity Theft Assistance Center.

She began her legal career with the Board of Governors of the Federal Reserve Board, where she was assistant director of the Division of Consumer and Community Affairs, and subsequently served as general counsel of CoreStates Bank of Delaware, the credit card subsidiary of CoreStates Financial Group. Ms. Wallace holds degrees from the Boston University School of Law and Fordham University.

Our final witness today is Ms. Susanna—and Susanna, help me with your surname.

Ms. MONTEZEMOLO. Montezemolo.

Mr. COBLE. Montezemolo. Ms. Montezemolo is a policy analyst in the Washington, D.C., office of Consumers Union, the nonprofit independent publisher of *Consumer Reports*. She serves as a public interest advocate on finance, privacy, and product safety issues. She holds a bachelor's degree in public affairs from the Woodrow Wilson School at Princeton University.

We are pleased, indeed, to have you all with us. Now as you all have been previously informed, we operate under the 5-minute rule. You will not be severely punished when that red light appears, but that is your warning to wind up. When the amber light

appears on the panel before you, that's your signal that you have 1 minute remaining.

Ms. Parsky, we will begin with you.

TESTIMONY OF LAURA H. PARSKY, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Ms. PARSKY. Thank you very much, Mr. Chairman. Good morning.

Good morning, Ranking Member Scott and other Members of the Committee.

I am pleased to be able to testify today to share with you the Department's view of the cyber-crime problem and how we have responded to that problem, and to discuss with you what we see as the legislative needs in this important area.

Where several years ago a hacker might have invaded the security of a business or Government agency simply for the thrill of breaking in, that individual is now much more likely to steal databases of personal information to sell to identity thieves on the black market.

Criminals also commonly use malicious spyware as part of "phishing" schemes in an effort to obtain financial information. Computer security experts estimated that in 2005 over $2 million—$2 billion were stolen through access to U.S. bank accounts.

The trend of computer crimes being driven by the allure of easy money is also evident in the growing prevalence of botnets. Essentially, a botnet is an army of compromised computers subject to the unauthorized control of an outsider.

Criminals have discovered many ways to exploit botnets for financial gain. Not only can these botnets be used to send illicit spam e-mails in a way that obscures their origin, but the botnets can also be used to execute or threaten to execute denial of service attacks on particular computers, including those of business competitors.

In response to this rapidly evolving problem, the President has personally shown great leadership. Just yesterday, he met with several victims of identity theft and signed an executive order creating an identity theft task force to marshal the resources of the entire Federal Government to crack down on identity theft. This task force will be chaired by the Attorney General, with the chairman of the Federal Trade Commission as co-chairman.

The Department of Justice has been working swiftly and decisively to address the growing threat of cyber-crime. For example, a year-long investigation by the Secret Service led to the indictment of U.S. and foreign members of the Shadowcrew organization.

This criminal organization created an online hub for identity thieves to buy and sell stolen identity information and stolen credit and debit card numbers. It also provided extensive information to its members about how to hack into computers, forge identity documents and credit cards, and commit fraud with stolen identity information.

The members of this one-stop online marketplace trafficked in at least 1.5 million stolen credit and bank card numbers, causing esti-

mated losses in excess of $40 million. To date, 17 defendants have pled guilty in this case.

In another successful prosecution, we convicted the perpetrator of the largest data theft in history. The defendant used sophisticated decryption software to obtain passwords and then used them to steal over a billion records containing personal information, such as physical addresses, e-mail addresses, and telephone numbers. The data was worth tens of millions of dollars. The defendant in this case, Scott Levine, was sentenced in the Eastern District of Arkansas to 96 months in prison.

We've also had notable success investigating crimes involving botnets. Since January, we have obtained the convictions of two major botmasters. In Seattle, Washington, an individual pled guilty to using a botnet in a fraud scheme that netted him over $100,000.

In operating this botnet, however, he damaged the computer system of a hospital. When the system went down, it affected the hospital systems in numerous ways. Doors of the operating rooms did not open. Pagers did not work. And the computers in the intensive care unit shut down. By reverting to backup systems, the hospital was able to avoid any harm to patients, but obviously, the consequences could have been much worse.

In addition, the FBI and the U.S. attorneys' office for the Central District of California secured the conviction of Jeanson James Ancheta, a well-known member of the botmaster underground, on charges related to his profitable use of botnets that were used to launch destructive attacks, to send huge quantities of spam e-mail across the Internet, and to receive surreptitious installations of adware.

Ancheta controlled over 400,000 computers, including some owned by the Department of Defense. As a result of his guilty plea to the criminal charges, Ancheta was sentenced this week to 57 months imprisonment.

While we continue aggressively to pursue these cyber-criminals, we believe that there are additional legislative tools that could assist us as the nature of their crimes evolves. I would like to sincerely thank this Committee for its attention to this important issue and its work in introducing H.R. 5318. We believe that this bill includes a number of important provisions, and we firmly support the bill's goals.

In my written statement, I've provided a number of comments on the bill and have highlighted a few ways that we think the legislation might be further strengthened. However, we intend to follow up with a views letter on behalf of the Administration that will provide a more comprehensive analysis and recommendations.

To highlight just one of our comments on H.R. 5318, let me express our strong support for section 3B of the bill, which cures a problematic loophole in the Computer Fraud and Abuse Act. This amendment would enhance our ability to investigate and prosecute hackers and identity thieves who steal information from computers.

Finally, I would like to note that my written statement includes additional suggestions for ways to improve the laws we use to combat computer and Internet crime. For example, it has at times proved difficult to prosecute offenders who install malicious soft-

ware on many computers when the harm to each computer is relatively slight.

Although the aggregate harm may be quite significant and rise above the current $5,000 threshold for Federal jurisdiction, it can be difficult to present evidence to each—evidence of each individual harm in court, calling as witnesses hundreds of computer owners.

This problem could be solved simply by lowering or eliminating the monetary threshold or by adding an additional trigger for Federal jurisdiction for this type of offense. In the next few days, we will provide the Committee with a comprehensive list of our proposals.

Again, I would like to thank the Subcommittee for the opportunity to testify here today. The threat of computer crime has an enormous impact on our Nation's economy and on the security and privacy of all our citizens.

Thank you. And I'd be happy to answer any questions.

[The prepared statement of Ms. Parsky follows:]

PREPARED STATEMENT OF LAURA PARSKY

Statement of Laura Parsky,
Deputy Assistant Attorney General
United States Department of Justice
U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime,
Terrorism and Homeland Security

Legislative Hearing on H.R. 5318, the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006"

May 11, 2006

Good morning, Mr. Chairman, Ranking Member Scott, and Honorable Members of the Subcommittee. I am very pleased to be able to testify today to share with you the Department's view of the cybercrime problem and how we have responded to that problem and to describe what we see as the legislative needs in this important area.

I. THE CYBERCRIME LANDSCAPE

I would like to begin by giving you some perspective on the threat cybercrime poses to our security, our privacy, and our economy. Through our investigations and prosecutions over the past several years, we have begun to see a pattern emerge: hackers who at one time might have broken into computers out of curiosity or for "bragging rights" have turned to exploiting that access for financial gain.

This trend can be seen in a number of areas. Where several years ago a hacker might have invaded the security of a business or government agency simply for the thrill of breaking in, that individual is now much more likely to steal databases of personal information to sell to identity thieves on the black market. Indeed, an underground economy has developed where criminals, often residing overseas, buy and sell credit card numbers and bank account information. Some of these identity thieves advertise the fact that they have access to literally

millions of stolen credit card records. Although law enforcement has made inroads into addressing this problem, it appears to be getting worse.

The profit motive is also apparent in the use of malicious spyware. In one recent prosecution in the Southern District of California, for example, a criminal defendant is alleged to have commercially marketed a program that any buyer could secretly send in an email attachment to an ex-girlfriend or an estranged spouse. Marketed as "loverspy," this program would intercept all of the communications of the person using that computer and send them to the person who bought the program. Five individuals have been indicted in the Southern District of California to date for selling or using this program. Four of these defendants have pled guilty and are awaiting sentencing. Additional convictions relating to this case have been obtained in federal courts in Charlotte, North Carolina, Dallas, Texas, and Honolulu, Hawaii. Additional indictments are pending in Kansas City, Missouri, and Houston, Texas.

Criminals also commonly use malicious spyware as part of "phishing" schemes - the sending of spam email messages to unsuspecting users in an effort to obtain their credit card numbers and other financial information. By appearing to be a message from the user's bank, some of these messages try to trick users into giving up their bank account numbers and passwords. Other phishing schemes cause spyware to be installed on the user's computer that grabs the user's information, intercepts the user's communications, and sends it all back to the criminal. Because it is so cheap to send out millions of phishing emails, even a success rate of less than 5 percent allows the criminals to commit widespread fraud. Computer security experts estimated that in 2005 over $ 2 billion were stolen through unauthorized access to U.S. bank accounts.

The trend of computer crimes being driven by the allure of easy money is also evident in the growing prevalence of "botnets." While five years ago viruses and worms were often disseminated just to destroy networks or to gain notoriety, today they are used to make money. For example, worms often illegally install a kind of malicious software called a "bot" on the victim's computer. These "bots" can gain complete control over the computer and report back for instructions to the person who sent them. Such "bot herders" can gain control over thousands of computers in this way, forming a "botnet" - a kind of clone army that can be deployed either individually or as a group. Symantec recently estimated that four million computers are currently infected with bots.

Clever criminals have figured out how to exploit botnets to make money. Bot herders can send illicit spam emails through bots, thus obscuring the origin of the spam and making it harder for Internet service providers to block. Of course, such spam can also include the phishing schemes mentioned above. Bot herders also earn money by causing advertising to appear on a bot-infected computer's screen. And perhaps most perniciously, botnets have the combined power to knock other computers offline. Companies have paid to have such "distributed denial of service attacks" (or "DDOS attacks") render their competitors' websites inoperable, and bot herders have extorted hundreds of thousands of dollars from businesses and individuals by threatening to do so. Computer security experts estimate that denial of service attacks occurred approximately 1,400 times a day in 2005.

Not surprisingly, bot herders have found an additional way to profit from this general-purpose criminal tool: they have rented and sold botnets to anyone willing to pay. By this means, botnets can fall into the hands of any criminal, even one without the technical skill to create a botnet.

Consistent with these patterns, surveys show that the number of breaches of computer security remains high. The 2005 report produced by the Computer Security Institute and the Federal Bureau of Investigation ("FBI") found that about seventy-five percent of respondents suffered attacks from computer viruses, such as those used to infect computers with "bots." The report also showed that the incidence of attacks on wireless computer networks has continued to increase. Finally, the report revealed that victims of computer crime are consistently failing to report such incidents to law enforcement. Indeed, reporting to law enforcement dropped to only twenty percent, the lowest level recorded in the ten years that the study has been conducted.

Moreover, these attacks on computer networks threaten the stability of our modern economy, which has become increasingly reliant on such networks, and threaten our national security. Many of our critical national infrastructures - such as transportation, electricity transmission, and banking and finance - rely on the security and reliability of computer network communications. Any disruption of these networks, whether it is through criminal activity or terrorist acts, can cause widespread harm. This reality makes it all the more critical that we be able to respond quickly to threats to these networks and appropriately deter such misconduct.

II. THE LAW ENFORCEMENT RESPONSE

In response to this rapidly evolving problem, the Department of Justice has worked swiftly and decisively to address these growing threats. The cornerstone of the Department's prosecutorial efforts is the Computer Crime and Intellectual Property Section, a highly trained team of 40 expert prosecutors who specialize in coordinating multi-district and international investigations of computer crime and intellectual property offenses.

The Computer Crime and Intellectual Property Section trains, supports, and works closely with Computer Hacking and Intellectual Property ("CHIP") prosecutors in each of the 94

U.S. Attorneys' Offices. CHIP prosecutors are specially trained in computer crime and intellectual property prosecutions, and they work both individually and together to ensure a strong and coordinated domestic enforcement effort. In addition to individual CHIP attorneys, there are now 18 CHIP Units throughout the country. The CHIP prosecutors, CHIP Units, and CCIPS work closely with the FBI, the U.S. Secret Service ("Secret Service") and the Bureau of Immigration and Customs Enforcement ("ICE") of the Department of Homeland Security, and other investigative agencies.

The FBI has made cybercrime, including fraud, hacking, child pornography, and intellectual property crime on the Internet, one of its top three enforcement priorities. To this end, the FBI has ensured there is a cyber expert in each of its 56 field offices, and in many of these offices the FBI has established special "cyber squads." Similarly, the Secret Service has an extensive program comprised of agents specializing in electronic crimes (the Electronic Crimes Special Agent Program or "ECSAP").

It is also important to understand that the science of computer forensics is of increasing importance in cybercrime investigations. New computers sold for use in the home routinely have hard drives which could store the entire contents of the Library of Congress. Business computers store much greater volumes of data. When these computers are searched as part of a criminal investigation, the government must have forensic tools and trained forensic examiners to sift quickly through this massive amount of data to search for evidence of a crime. They must also be thoroughly familiar with where data can be hidden on a hard drive and how to use the Internet to recreate the trail of hackers and identity thieves that can operate from anywhere in the world. Furthermore, because many state and local law enforcement agencies do not have adequate computer forensic resources, the federal government is increasingly called upon to

provide forensic assistance in a broad variety of crimes prosecuted at that level. In order to provide greater assistance to state and local law enforcement, the FBI, through its Regional Computer Forensics Laboratories, and the Secret Service, through its Electronic Crimes Task Forces, have provided assistance and training to hundreds of local investigators.

All of these efforts have led to a number of important prosecutions. For example, a year-long investigation by the Secret Service led to the indictment of 27 U.S. and foreign members of the "Shadowcrew" organization in October 2004. Shadowcrew and its associated website, www.Shadowcrew.com, created an online hub for identity thieves to buy and sell stolen identity information and stolen credit and debit card numbers. It also provided extensive information to its members about how to hack into computers, how to make fraudulent identity documents and credit cards, and how to use stolen identity information to commit fraud. The members of this one-stop online marketplace trafficked in at least 1.5 million stolen credit and bank card numbers. Victims estimated losses in excess of $40 million. To date, 17 defendants have pled guilty in the case.

In addition, in the Eastern District of Arkansas, the Department of Justice, the FBI, and the Secret Service investigated and convicted the lead defendant of the largest data theft in history. At trial, the Government showed that between January and July of 2003, Scott Levine used sophisticated decryption software illegally to obtain passwords and then used those passwords to steal over a billion records containing personal information, such as physical addresses, email addresses, and telephone numbers. The data was worth tens of millions of dollars. The jury convicted Levine of 120 counts of unauthorized access to a protected computer. In February of this year, a federal judge in Little Rock, Arkansas, sentenced Levine to 96 months in prison.

In another recent case in the Northern District of California, a former manager of a debt collection company was convicted for using a computer code "time bomb" to corrupt the customer data base of his former employer. When the manager learned that he was facing dismissal, he designed and installed malicious code that would activate at a time after he left the company. The malicious code then deleted and modified financial records relating to over 50,000 customer accounts and caused over $100,000 in damages. The defendant was convicted after a jury trial and is currently awaiting sentencing.

We have also had some notable successes in investigating crimes involving botnets. In one recent case in Seattle, Washington, an individual pled guilty to using a botnet in a fraud scheme that netted him over $100,000. In the process of expanding the number of compromised computers in this botnet, however, he damaged the computer system of a hospital. When the system went down, it affected the hospital's systems in numerous ways: doors to the operating rooms did not open, pagers did not work, and computers in the intensive care unit shut down. By reverting to back up systems, the hospital was able to avoid any harm to patients, but obviously the consequences could have been much worse. The defendant is currently awaiting sentencing.

In addition, in the first prosecution of its kind in the nation, the FBI and the U.S. Attorney's Office for the Central District of California secured the conviction of Jeanson James Ancheta, a well-known member of the "botmaster underground," on charges related to his profitable use of botnets that were used to launch destructive attacks, to send huge quantities of spam email across the Internet, and to receive surreptitious installations of adware. Through his crimes, Ancheta controlled over 400,000 computers, including some computers owned by the Department of Defense. In addition to his guilty pleas to the criminal charges, Ancheta agreed to pay roughly $15,000 in restitution to the Weapons Division of the United States Naval Air

Warfare Center in China Lake and the Defense Information Systems Agency, whose national defense networks were intentionally damaged by Ancheta's malicious code. Ancheta was sentenced this week to 57 months' imprisonment and was ordered to forfeit his ill-gotten gains, including $60,000 in cash and his BMW automobile.

The Department's efforts to fight cybercrime do not stop at America's borders. Just as the Internet is unfettered by national boundaries, so Internet crime almost invariably involves computers, electronic evidence, and defendants across the globe. Indeed, even domestic criminals preying on domestic victims can route their communications through overseas networks, requiring the assistance of foreign law enforcement agencies to solve what is in essence a domestic crime.

Recognizing these difficulties, the Department has promoted international law enforcement capabilities and has assisted foreign lawmakers in modernizing their cybercrime laws. These efforts will enable foreign law enforcement to gather electronic evidence that is important to U.S. investigations, as well as to investigate and prosecute offenders in their own countries. For example, the U.S. Department of Justice has spearheaded efforts in the Group of Eight ("G8") to ensure that the world's eight major industrial economies have strategies and policies in place to fight cybercrime. Through this forum, we have created and led a network of high-tech law enforcement agencies from 43 nations that is now able to respond to urgent Internet crimes 24 hours a day, seven days a week.

In addition, the Department was an active participant in the negotiation of the historic Convention on Cybercrime (2001). The Convention on Cybercrime is essential to securing the international cooperation necessary to enforce our criminal and intellectual property laws and to protect the Nation and the critical information infrastructures of our commercial,

communication, and defense sectors. At the same time, it fully preserves existing protections regarding the rights and privacy of individuals. Ratification of the Convention is a top priority of this Administration. In the absence of the Convention, we may find ourselves unable to obtain critical computer evidence from overseas that might allow us to prevent a new terrorist attack, or to break up an international pedophile ring, or to prosecute those who defraud our fellow-citizens from locations abroad. Now under consideration for the advice and consent of the Senate to ratification, this first-of-its-kind treaty will promote our worldwide efforts to address such online crimes as computer hacking, Internet fraud, child pornography, and intellectual property theft.

III. THE NEED FOR LEGISLATIVE ACTION - COMMENTS ON THE COMPUTER SECURITY ENHANCEMENT AND CONSUMER DATA PROTECTION ACT OF 2006

Let me turn now to our own legal framework. As a result of Congressional efforts over the past ten years, federal laws available to combat cybercrime have improved significantly. However, we believe that Congressional action in several particular areas would improve our ability to investigate and prosecute these offenses. In particular, we recommend that Congress strengthen the penalties for computer hacking, close loopholes in certain criminal statutes, and clarify the scope and applicability of the laws that govern the collection of electronic evidence.

On May 1, 2006, the Department received a draft bill entitled, "The Computer Security Enhancement and Consumer Protection Act of 2006." This legislation, introduced this past Tuesday as H.R. 5318, includes a number of important provisions, and we firmly support the bill's goals. I would like sincerely to thank the Committee for its attention to this important issue and hope to highlight for you some of the ways we think the bill might be further strengthened. . I will touch on a few of these today with you. We intend to follow up with a views letter on behalf of the Administration that will provide a more comprehensive analysis and recommendations.

A. Section 3 - Theft of Information from Computers

We strongly support Section 3(b) of the bill that cures a problematic loophole in the Computer Fraud and Abuse Act (18 U.S.C. § 1030). This amendment would enhance our ability to investigate and prosecute hackers and identity thieves who steal information from computers. Under current law, federal courts only have jurisdiction over the theft of information from a computer if the criminal uses an interstate communication to access that computer (except if the computer belongs to the federal government or a financial institution). Yet in many cases criminals steal data through purely in-state actions. For example, corporate employees can exceed their authorization to access vast numbers of electronic records. Similarly, individuals often plant spyware programs on the computers of people they know in order to obtain their private communications and passwords.

Moreover, the advance of wireless technology has made the current provision outmoded. In one case in North Carolina, for example, an individual broke into a hospital computer's wireless access point and thereby stole patient records. State investigators and the victim asked the United States Attorney's Office to support the investigation and charge the criminal; however, because the communications occurred entirely intrastate, it did not violate the Computer Fraud and Abuse Act.

Section 3(b) corrects this significant loophole. This amendment will allow federal investigators and prosecutors to pursue intrastate theft of information without requiring proof that the conduct involved an interstate communication. Federal jurisdiction under the amended statute would be based, as it is in most other subsections of the Computer Fraud and Abuse Act,

on the fact that the victim computer itself is used in interstate or foreign commerce or communications.

B. Section 4 - Use of Computer Hacking by Organized Crime

Section 4 of the bill would make the Computer Fraud and Abuse Act a predicate offense for violations of the Racketeering Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1961 et seq., a charge used to prosecute organized crime groups and other criminal enterprises. We support this amendment but would recommend limiting it to the felony subsections of Section 1030 to ensure that it will apply only to the more serious hacking offenses.

As organized crime groups begin to turn to the Internet to commit such traditional crimes as fraud, money laundering, and gambling, and as hackers are increasingly motivated by the desire for financial gain, the activities of these criminal elements will increasingly overlap. Thus, it makes sense to include elements of the Computer Fraud and Abuse Act as RICO predicates.

The following fact patterns illustrate the involvement of criminal enterprises in the more serious types of violations of Section 1030:

- Section 1030(a)(2) (Theft of Information). Criminal enterprises have been tied to large-scale online thefts of credit card numbers and other financial information from banks and credit card processors. The investigation of the Shadowcrew organization described above is an example of such a criminal enterprise.

- Section 1030(a)(4) (Computer Hacking as Part of a Fraud Scheme). Organized criminal groups have used "phishing" attacks to place spyware on computers to gather users' financial information, credit card numbers, and similar information. For example, Brazilian authorities recently arrested over 50 individuals involved in a sophisticated, organized phishing ring that used spyware to steal roughly $66 million from online-banking customers. Under U.S. law, this sort of scheme would violate Section 1030(a)(4).

- Section 1030(a)(5) (Damage to Computers or Information). Criminal enterprises appear to be involved in the creation of botnets that can be used to launch denial of service attacks against online commercial activities. In at least two instances over the last two years, the Department has charged business owners for paying others to conduct distributed denial of service attacks on business competitors for commercial advantage.

- Section 1030(a)(7) (Extortion by Threatening to Damage Computers or Information). Criminal enterprises are committing extortion by threatening to disrupt online commercial activities. For example, British and Russian police have broken up several extortion rackets that targeted online gambling sites in the United Kingdom and the Caribbean.

As these examples demonstrate, criminal enterprises increasingly are finding ways to commit fraud and related criminal activities through and against computers, and they are doing so in ways that make it more difficult to prosecute the offenders using traditional conspiracy charges. Therefore, adding felony violations of the Computer Fraud and Abuse Act to the list of RICO predicates in Section 1961(1) would ensure that we have the necessary and appropriate tools to address evolving trends in cybercrime committed by criminal enterprises.

C. Section 5 – Cyber-Extortion

Section 5 of the bill amends the law relating to cyber-extortion. We appreciate the Committee's recognition of the importance of this provision, especially given current trends in cybercrime, as discussed above, and its recognition that the existing law has certain shortcomings; however, we recommend a different approach to addressing these shortcomings. Existing section 1030(a)(7), which governs threats to damage computers or information, does not cover certain types of extortion schemes that have come to our attention. For example, some cybercriminals extort companies without explicitly threatening to cause damage to computers. Instead, they steal confidential data and then threaten to make that data public if their demands are not met. Others cause the damage first – such as by accessing a corporate computer without authority and encrypting critical data – and then threaten that they will not correct the problem

unless the victim pays. These types of extortion should be covered by the Computer Fraud and Abuse Act, but we recommend covering such acts more explicitly. The Department will be glad to provide the specific language we recommend to address this issue.

D. Section 7 - Notice to Law Enforcement

Section 7 would require notifying law enforcement when a security breach of a system containing personal information occurs. We strongly support the goal of this provision, and we believe the language requiring prior notification to the Secret Service or the FBI will allow for appropriate law enforcement investigation of unauthorized access to personal information. Without such reporting, we cannot ensure that we are effectively punishing those who have committed these destructive crimes and deterring those who might do so in the future.

We have several suggestions, however, to improve the language:

1. Proposed Section 1039(a) (Section 7(a) of H.R. 5318)

This provision would only require law enforcement notification where the breach "causes economic harm to any person." We recommend striking this clause. If any type of security breach occurs - even one where prompt action prevented harm, there should be an appropriate law enforcement investigation. It is only through such investigations that the criminals can be identified and their conduct deterred. Moreover, in many cases, it may be difficult for the victim of the security breach to determine whether or not economic harm has occurred. Months might pass, for example, before it is determined that stolen personal information was used to commit identity theft. Notification in such cases should not turn on whether the victim can prove that economic harm has occurred. Further, even in those cases where there is no economic harm, the unauthorized access results in a breach of the confidentiality of personal information. Such privacy violations alone justify law enforcement action.

2. Proposed Section 1039(b)

We recommend that the scope of the definition of "major security breach" in this section be clarified to include any breach of the security of personal information. The Department would be pleased to work with the Committee on specific language.

E. Section 8 - Penalties for Section 1030 Violations

Section 8 accomplishes two goals: it increases the penalties for computer crimes, and it allows for forfeiture of the fruits and instrumentalities of computer crime. Let me address these points in order.

1. Criminal Penalties

First, Section 8 would eliminate the complex sentencing scheme for the various subsections of the Computer Fraud and Abuse Act and create a single overarching maximum penalty of 30 years in prison. While we believe that there are ways to strengthen the sentencing for offenses under Section 1030 and make the sentencing scheme less complex, we believe it is important to maintain a sentencing scheme that is tailored to the different gradations of harm caused by these offenses.

Unquestionably, there is a need for strong deterrence against computer hacking violations, and we recommend increasing the sentences for particularly harmful offenses. For example, the penalties for the theft of information (Section 1030(a)(2)) have become inadequate in light of the rise of identity theft, "phishing," and spyware activity. Under current law, obtaining information from another person's computer without authorization is generally a misdemeanor offense with a maximum penalty of one year in prison. 18 U.S.C. § 1030(a)(2)(C), (c)(2)(A). The offense becomes a 5-year felony only if the actor committed the violation for

financial gain, in furtherance of another crime or a tort, or if the value of the stolen information exceeds $5,000.

These statutory bases for an increased penalty do not take into account the serious privacy invasions that occur without a financial motive, such as when spyware programs steal the sensitive, private information of a computer user, and the person installing the spyware is motivated by revenge or prurient interest. Currently, these invasions of privacy do not constitute felony offenses, and the existing misdemeanor penalty does not create an adequate punishment or deterrent. Further, even when one of the aggravating factors listed in the statute is present, such as when the crime is committed in furtherance of a fraud scheme, the current five-year maximum sentence is not commensurate with the gravity of the harm caused. Thus, we recommend raising the maximum penalty for these offenses to 3 years' imprisonment for ordinary offenses under Section 1030(a)(2) and to 10 years' imprisonment where the actor committed the violation for financial gain, in furtherance of another crime or a tort, or if the value of the stolen information exceeds $5,000.

2. Forfeiture

Second, Section 8 also addresses the forfeiture of computers used in hacking crimes. Under current law, the Government can seek forfeiture of the proceeds of violations of the Computer Fraud and Abuse Act but not of the instrumentalities used to commit such crimes. While Section 8 seeks to address this shortcoming in the current forfeiture regime, we recommend adding text to clarify the procedure to be used in forfeiture proceedings. In addition, civil forfeiture is extremely important in cases of this nature, because the defendants may be overseas and thus beyond the reach of a criminal prosecution. Thus, we suggest adding a section

to allow for civil forfeiture. We would be happy to recommend to the Committee specific language for these provisions.

III. ADDITIONAL LEGISLATIVE PROPOSALS

In addition to our comments on the Cyber Security Enhancement and Consumer Data Protection Act of 2006, I would like to share with you some additional suggestions for ways to improve the laws we use to combat computer and Internet crime. I will touch on a few of these suggestions, and the Department will provide the Committee with a comprehensive list of our legislative proposals.

A. Enhancing the Prosecution of Attacks on Computers

As a result of recent investigations and prosecutions, we have discovered that the laws criminalizing attacks on computers contain several limitations that have made it more difficult to prosecute certain criminal conduct. For example, it has at times proved difficult to prosecute offenders who install malicious software on many computers when the harm to each computer is relatively slight. Although the aggregate harm may be quite significant and rise above the current $5,000 threshold for federal jurisdiction, it can be difficult to present evidence of each individual harm in court without calling as witnesses hundreds of computer owners. This problem could be solved simply by lowering or eliminating the monetary threshold or by adding an additional trigger for federal jurisdiction for this type of offense.

In addition, 18 U.S.C. § 2701, the law prohibiting unauthorized access to another's email, should be clarified to ensure that it protects all email. As currently drafted, this statute may only apply to email that has not yet been received by the intended recipient. A simple amendment would clarify Section 2701 to allow prosecution of criminals who harm the privacy of others by accessing their email, whether unread or read and then stored.

B. Clarifying the Procedures for Responding to Foreign Requests for Electronic Evidence

Under current law, the United States is generally able to provide assistance to foreign law enforcement agencies that are investigating computer crimes. Providing such assistance is particularly important, because it allows us to fulfill our obligations under various treaties, and because it creates the environment in which U.S. law enforcement agencies can, in turn, obtain assistance from foreign law enforcement agencies. Moreover, even to solve domestic computer crimes, it is often necessary to obtain some electronic evidence from overseas in order to identify and prosecute the offenders. Only by providing assistance to foreign law enforcement authorities can we expect to receive assistance where the crime involves an American victim. Thus, our ability to provide assistance to foreign investigators has a direct impact on the safety and security of Americans.

However, the statutes that govern the obtaining of electronic and other evidence based upon a foreign request contain certain ambiguities. With respect to electronic evidence, in 2001, Congress changed the wording of 18 U.S.C. § 2703 in a way that inadvertently introduced confusion in routine mutual legal assistance cases. For example, Section 2703(a) requires that the court issuing a search warrant for stored electronic evidence have "jurisdiction over the offense." Since a U.S. court often has no jurisdiction to try a foreign offender, the wording of Section 2703(a) needlessly complicates the use of this type of court process. Therefore, we recommend clarifying the definition of "court of competent jurisdiction" in section 2711.

IV. CONCLUSION

In conclusion, I would like again to thank the Subcommittee for the opportunity to testify here today. The threat of computer crime has an enormous impact on our nation's economy and on the security and privacy of all of our citizens. The Department is firmly committed to

addressing this threat by aggressively investigating and prosecuting these offenses and to deterring future offenders by seeking appropriately severe sentences. Congressional action now will significantly improve our ability to address the growing threat of cybercrime.

I would be happy to answer any questions that the Subcommittee may have. Thank you.

Mr. COBLE. Thank you, Ms. Parsky.
Mr. LaRocca.

TESTIMONY OF JOSEPH LaROCCA, VICE PRESIDENT, LOSS PREVENTION, NATIONAL RETAIL FEDERATION

Mr. LAROCCA. Thank you, Mr. Chairman.

And good morning, Ranking Member Scott and other Members of the Subcommittee.

My name is Joe LaRocca. I'm the vice president of loss prevention with the National Retail Federation. We're a trade group based here in Washington, representing all retails, all sectors of retail.

And I'm here today to testify about the Cyber-Security Enhancement Consumer Protection Act of 2006, H.R. 5318.

The NRF applauds the Committee for initiating this effort to acknowledge and address the growing problem of cyber-crime, and the bill before you is a good first step toward punishing and deterring the bad actors, while also protecting the interests of our consumers and our businesses.

With over 18 years of experience in the retail loss prevention and operations field, I speak from a lot of experience—from personal experience as well as experiences of my colleagues—about the issues that have faced us in the past, such as physical thefts, like shoplifting, embezzlement, vandalism, and potential acts of terrorism against retail establishments.

But now a new era is here with online and computer intrusion acts that cost companies billions of dollars, cost consumers billions of dollars, and make us both victims. Cyber-crime is an increasingly destructive form of trespassing.

For example, in November 2003, three men accessed the computer system of a large, well-known home improvement retailer. They installed programs, or bots, on the computer systems of several stores and ultimately conspired to hack the retailer's central communication system in North Carolina. Years earlier, one of the individuals at age 17 faced charges for allegedly hacking into an Ann Arbor, Michigan, nonprofit Internet company.

In 2004, a Boston-based warehouse club was the victim of cyberthieves. In response to banks—in response, banks sent hundreds of thousands of replacement credit cards to consumers across 16 States.

In April 2005, a well-known New York-based specialty retailer reported a systems breach resulting in 180,000 elements of credit card data being compromised. And in March 2005, a large Columbus-based shoe warehouse chain reported the theft of credit card and personal shopping information for 170,000 of its customers.

These were the cases that were widely reported. Most security experts agree that a large number of hacking incidents go unreported due to the negative publicity of doing so or the fear of future attacks.

Unauthorized access and use of the retailer customer data is really a double hit, first to our customers, then to us, the retailer. These rare and unfortunate circumstances happen, but we join with our customers as victims of smart and often distant cyber-

criminals who are just seeking out the thrill or the biggest security hack they can perpetrate.

Even when retailers are not the direct target, there is still a significant risk for our industry. When hacking incidents or consumer records are fraudulently obtained from companies like ChoicePoint, Axium, Bank of America, University of Southern California, and LexisNexis, the data obtained by these cyber-criminals is often used to commit other crimes, such as opening credit accounts and using true name fraud or assuming the identity of legitimate consumers and making fraudulent purchases, costing consumers and retailers in excess of $50 billion annually.

And while my examples are focused on the financial impact to retailers, we cannot forget that many of these computer intrusions result in lost data, system downtime, and lost hours of work for employees and companies that must then undergo significant review, recovery, and overhaul of their technical infrastructure.

Quoting FBI director Mueller from testimony given to the Senate Committee on Intelligence in February of last year, "The cyber-threat to the United States is serious and continues to expand rapidly the number of actors with both the ability and the desire to utilize computers for illegal and harmful rises. Terrorists show a growing understanding of the critical role that information technology plays in the day-to-day operations of our economy and national security."

He goes on to say that the growing number of hackers motivated by money is a cause for concern. If this pool of talent is utilized by terrorists, foreign Governments, or criminal organizations, the potential for such—for successful cyber-attack on our critical infrastructures is greatly increased.

Cyber-crime is a high reward, but a high risk business. And while some of the items are fraudulently purchased for the hacker, their family, or their friends, oftentimes these products are fenced, sold, or swapped through online auction sites and converted to cash. We call this activity "e-fencing."

Unfortunately, these purchases not only have a serious financial impact on businesses, this activity results in lost sales, as honest consumers are not able to purchase the most desirable goods a retailer can stock.

On behalf of the National Retail Federation, its members and businesses and consumers, I'd like to thank the Committee for having me here today, the development of this H.R. 5318. And I'm happy to answer any questions you or the Committee may have.

[The prepared statement of Mr. LaRocca follows:]

PREPARED STATEMENT OF JOSEPH LAROCCA

Good morning Chairman Coble, Ranking Member Scott and members of the Subcommittee. My name is Joe LaRocca. I am the Vice President of Loss Prevention for the National Retail Federation (NRF), in Washington, D.C. I am here to provide the retail community's perspective on H.R. 5318, the Cyber-Security Enhancement and Consumer Data Protection Act of 2006, being considered by this subcommittee. NRF applauds the subcommittee for initiating this effort to acknowledge and address the growing problem of computer-based, or "cyber" crime, we agree it is appropriate that efforts first be directed at updating current law—Title 18 Section 1030(a)(2) (aka, 18 U.S.C. 1030)—as is the focus of this bill, and NRF believes that the bill before you is a good first step toward punishing and deterring the bad actors while also protecting the interests of business and our customers.

The National Retail Federation is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet, independent stores, chain restaurants and grocery stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.4 million U.S. retail establishments, more than 23 million employees—about one in five American workers—and 2004 sales of $4.1 trillion. As the industry umbrella group, NRF also represents more than 100 state, national and international retail associations. *www.nrf.com.*

RETAILERS ARE VICTIMS OF COMPUTER CRIME

With over 18 years of experience as a loss prevention professional inside retail companies, I speak from experience about the significant and sweeping change I myself and colleagues of mine in loss prevention ("LP") have encountered and had to adapt to in order to stay ahead of the bad guys. What used to be a focus of our time and resources on physical crime—property based theft, embezzlement, etc.,—have quickly shifted and accelerated into the online world, presenting me and my colleagues with an entirely new, more sophisticated, harder to find, next to impossible to identify or reach culprit—the cyber-criminal.

Cyber-crime is an increasingly destructive form of trespass. The stakes grow higher by the day, as do the costs and measures needed to adequately secure retail websites, payment systems and databases in addition to our biggest asset, namely, our reputation. While LP activities have traditionally centered on losses within the store or our supply chain of goods, LP professionals are taking on greater responsibility for protection of our business brand. In retail, our customers not only want a good deal for a desirable item we sell, our customers need to TRUST us in order for our relationship to flourish. To protect and hold customer information close is a necessity for a competitive retailer, it simply makes no practical or economical sense for retailers to be blasé when it comes to customer TRUST or data security. Unauthorized access and use of retailers' customer data is a double hit—first to our customers, but also to retailers themselves. These rare and unfortunate circumstances happen, but we join with our customers as VICTIMS of smart and often distant cyber-criminals who are often just seeking out the thrill of the biggest security hack they can perpetrate, however, the minute customers stop trusting a retailer with their personal information, that retailer is doomed to fail. To protect ALL our assets (property, goods, employees, credit card information and brand), retail LP professionals are aggressively building bridges across our discipline and to law enforcement, and looking for tools to help us in our mission.

The advent of the Web is both a blessing and a curse for retail loss prevention. While our e-commerce divisions have exploded in recent years, retail losses have also grown. Considering that one of the original purposes of 18 U.S.C. 1030 as amended in 1996 was to protect credit card numbers and other financial data, it makes sense that ten years later a number of "updates" are needed in order to keep step with the trends and growth of new avenues of cyber-crime. For retailers to stay profitable and viable and keep our brands from irreparable harm, we need updated laws like H.R. 5318 to help defend our property and ultimately our customers.

COMMENTS ON H.R. 5318 AMENDMENTS TO CURRENT LAW 18 U.S.C. 1030

When last the federal computer crimes law was amended, Internet access and usage was still in its infancy. As the Internet grew, e-retailing with all its related benefits has also grown substantially. Likewise, smart criminals have kept on top of, or many times ahead of, technology trends. Their stealth activity is harder to detect, but not impossible, assuming law enforcement is provided with the right tools, and victims of computer crime have additional avenues to identify and prosecute those that perpetrate our loss or harm. While the retail community continues to reflect on the appropriate security measures and tools we must adopt across the industry, we are pleased to see this draft bill moving to help protect law-abiding stakeholders, and would like to comment on a few key provisions in H.R. 5318.

Given the seamlessness of the Web, it is vitally important that Section 3 of the bill before you seeks to broaden the scope of 18 U.S.C. 1030 to apply to foreign and interstate computer frauds, as we know the crime can be initiated from remote locations and can still have a direct and crippling impact on broad-based businesses that operate across jurisdictions and in the ether known as the Internet.

NRF also applauds the enhanced tools for law enforcement found in H.R. 5318. First, the Section 4 language to add 18 U.S.C. 1030 to the definition of "racketeering activity," as a Racketeer Influenced and Corrupt Organizations ("RICO") predicate offense to 18 U.S.C. 1961. Second, the Section 6 creation of a new federal offense

of "conspiracy to commit cyber-crimes," as so much of the computer-based crime is both organized and far more sophisticated in its execution. And finally the increased investigative and prosecutorial funding for federal law enforcement found in Section 10.

As for the penalties found in Section 8, it is laudable to see that the bill increases convictions of cyber-crime from 10 or 20 years to 30 years, as well as providing for stiffer forfeiture provisions. Expansion of these terms of imprisonment and tightening of property forfeiture is not only an incentive to law enforcement, but should prove to be a deterrent to all but the boldest of thieves.

SUMMATION

NRF is encouraged by the intent of H.R. 5318 bill and applauds the expansion of scope of 18 U.S.C. 1030, particularly its RICO predicate, the expanded funding for law enforcement, the establishment of a new conspiracy crime section, and its penalty enhancements. Likewise, on behalf of the National Retail Federation, its member retailers and my colleagues in loss prevention, I look forward to working with members of the subcommittee toward development and passage of updated, substantive and enforceable laws that further protect businesses and consumers from online fraud—particularly the growing trend of e-fencing—a phenomenon booming on auction sites and swap-lists across the Internet.

Mr. Chairman, I appreciate the invitation to come and address you and the subcommittee members on the merits the draft Cyber-Security Enhancement and Consumer Data Protection Act of 2006, and I welcome any questions or comments you may ask.

Thank you for your kind attention.

Mr. COBLE. Thank you, Mr. LaRocca.

Ms. Wallace.

TESTIMONY OF ANNE WALLACE, EXECUTIVE DIRECTOR, IDENTITY THEFT ASSISTANCE CORPORATION

Ms. WALLACE. Good morning, Chairman Coble and Ranking Member Scott.

I'm Anne Wallace, executive director of the Identity Theft Assistance Corporation. On behalf of our members, which include some of the Nation's largest financial services companies, I want to thank you for the opportunity to testify on these critical issues and to tell you about the Identity Theft Assistance Center.

Without commenting specifically on your legislation, we do applaud your efforts to ensure that any business that has personally identifiable information takes the protection of that information seriously.

Turning to identity theft, we all know that identity theft is not new. The Bible tells us how Jacob stole Esau's identity in order to get the blessing of his father, Isaac. However, most identity thieves are in it for the money. Their methods have changed dramatically over the years, and they continue to evolve rapidly.

In the 19th century, outlaws used guns and horses to rob stagecoaches, and people still rob banks today because there is money there. Increasingly, however, personal information is the key that unlocks value. Identity thieves still use old-fashioned methods, such as cunning, to separate consumers from personal information, but they also use dumpster diving, hacking, and sophisticated online schemes, including "phishing."

Two and a half years ago, the financial services industry and its professional association, the Financial Services Roundtable, came together to address the needs of victims and the needs of law enforcement. The Identity Theft Assistance Center, or ITAC, was de-

signed to give victims the help and peace of mind they need at this difficult time.

ITAC also helps law enforcement by sharing information about verified cases of identity theft from many companies located all over the country. Let me briefly describe the ITAC service.

The process starts at an individual ITAC member company. The consumer and that member company resolve any problems that may exist at that particular company. And if the problem involves identity theft, the consumer is offered the opportunity to use the ITAC service, which is free of charge to the consumer.

Then at ITAC, ITAC walks the consumer through their credit report to identify any suspicious activity. ITAC notifies the affected creditors and places fraud alerts with the credit bureaus. Since opening its doors in August of 2004, ITAC has helped more than 6,000 consumers restore their financial identity.

Now, at the beginning of the ITAC process, consumers are informed about ITAC's partnership with law enforcement and asked to consent to the sharing of information. This disclosure and consent process is the foundation of our information sharing with law enforcement.

In 2005, ITAC signed a data sharing agreement with the United States Postal Inspection Service, under which we provide on a weekly basis information about victims and the circumstances of the identity theft. The Postal Inspection Service loads this data into their financial crime database so it can be used by postal inspectors all over the country.

Also last year, we signed a data sharing agreement with the Federal Trade Commission under which we send the same data each week to the FTC, where they add it to their Consumer Sentinel database. As I'm sure you know, about 1,400 State, local, and Federal law enforcement agencies have access to the Consumer Sentinel database. We also work closely with FBI and Secret Service, who have 24-hour online access to Consumer Sentinel.

Now these are landmark agreements. Now in the past, many financial services companies shared data on an individual basis with their own cases with local law enforcement. This one-on-one sharing continues today and is very important. But ITAC's data sharing is unique because the information that we share with law enforcement represents verified cases of identity theft from many different companies. It's national in scope, and it's delivered in a consistent format.

ITAC data gives law enforcement a 360-degree perspective. Is there a single victim? Are there multiple victims? Is the perpetrator operating in the United States? Are they operating offshore? How are the crooks using the proceeds? Are they buying big screen TVs, or are they financing terrorism? ITAC data can help law enforcement answer these questions.

Our law enforcement partners tell us that the data they are getting from ITAC is helping them catch and prosecute identity thieves. The Postal Inspection Service recently told us that the ITAC data had been used in more than a dozen cases where suspects have been identified and, in some cases, arrested.

With data sharing established at the Federal level, we are moving to forge partnerships at the local and regional level where the

cases really are investigated and prosecuted. Just last week, we signed a data sharing agreement with the Regional Identity Theft Network, which is led and has been developed by the U.S. Attorney of the Eastern District of Pennsylvania.

We're also moving forward with analysis of the ITAC data. With more than 6,000 records in our database, we are reaching a critical mass, a point at which we can begin to map trends and patterns, which we hope will help member companies and law enforcement detect and prevent identity theft.

Thank you, Mr. Chairman, and I'll be happy to answer your questions.

[The prepared statement of Ms. Wallace follows:]

PREPARED STATEMENT OF ANNE WALLACE

Testimony of

Ms. Anne Wallace

On behalf of

The Identity Theft Assistance Corporation

To The

Subcommittee on Crime, Terrorism and Homeland Security

Committee on the Judiciary

May 11, 2006

Chairman Coble and Ranking Member Scott, I am Anne Wallace, executive director of the Identity Theft Assistance Corporation. On behalf of our members – which are some of the nation's largest financial services companies – I want to thank you for the opportunity to testify on critical issues related to information security. I also appreciate the opportunity to tell you about the Identity Theft Assistance Center, an innovative, collaborative initiative of the financial services industry that helps victims of identity theft restore their financial identity and partners with law enforcement to catch and convict the criminals.

Without commenting specifically on your legislation, we applaud your efforts to ensure that any business that has personally identifiable information take the protection of that information seriously. In general, we support a uniform national standard for security and customer notice, like that provided in the H.R. 3997, legislation reported by the House Committee on Financial Services. In addition, we support the following principles:

- Preservation of the security standards articulated in Title V of Gramm-Leach-Bliley;
- Exclusive enforcement by functional regulators for firms that are regulated under Gramm-Leach-Bliley and the Fair Credit Reporting Act; and
- Notice based on a "risk of identity theft" whether that notice is to consumers or law enforcement

While some breaches have occurred at financial firms, the vast majority have occurred in other sectors. We believe this is largely due to the fact that financial

services companies work very closely with their regulators to implement policies and procedures to safeguard customer data. Any additional legislation should complement Gramm-Leach-Bliley and the Fair Credit Reporting Act (and FACT Act amendments), not replace them.

Turning to identity theft, we all know that identity theft is not new. The Bible tells how Jacob stole Easu's identity in order to get the blessing of his father, Isaac. However, most identity thieves are in it for the money. Their methods have changed dramatically, and continue to evolve rapidly. In the 19th century, outlaws used guns and horses to rob stage coaches, and people still rob banks today because there is money there. Increasingly, however, personal information is the key that unlocks value whether that value is in the form of a credit card or health care services that the identity thief obtains using another person's identity. Identity thieves still use old-fashioned cunning to separate consumers from valuable personal information but they also use dumpster diving, hacking, and sophisticated online schemes such as "phishing."

The distinction is often made between violent crimes and nonviolent crimes like identity theft. Identity theft is not life threatening but its impact on victims and on society should not be underestimated. Identity theft is a vicious crime that can terrify victims, robbing them of their time and peace of mind as well as their money. Thanks to federal and state consumer protection laws, consumers usually recover most of the money stolen by the thief with industry bearing much of the upfront financial cost, estimated in the hundreds of millions of dollars. But consumers suffer the emotional consequences of the crime, and may spend years restoring their credit and identity.

Consumers also are angry and frustrated by the fact that relatively few identity thieves are prosecuted and convicted. Two problems – the small dollar amount of most cases and jurisdictional boundaries – allow identity theft gangs to exploit information gaps between law enforcement agencies. Because there is no central aggregation of identity theft information reported by victims and merchants, small thefts committed in multiple jurisdictions or reported to various local, state or federal agencies, are not connected to similar thefts to reveal the workings of these gangs. One police department investigating a gang will have little chance finding out whether any other agencies are investigating the same gang.

Two and a half years ago, the financial services industry and its professional association, The Financial Services Roundtable and BITS, came together to address the needs of victims and the needs of law enforcement. The Identity Theft Assistance Center, or ITAC, was designed to give victims the help and peace of mind they need at this difficult time. ITAC also helps law enforcement by sharing information about verified cases of identity theft from many companies located all over the country.

Let me briefly describe ITAC's victim assistance service. The process begins at an individual ITAC member company. The consumer and the member company resolve any issues at that company and, if the problem involves identity theft, the consumer is offered the ITAC service free of charge. Then, ITAC walks the consumer through his or her credit report to identify suspicious activity. ITAC notifies the affected creditors and places fraud alerts with the credit bureaus.

Since opening its doors in August 2004, ITAC has helped more than 6,000 consumers restore their financial identities.

At the beginning of the ITAC process, consumers are informed about ITAC's partnership with law enforcement and asked to consent to the sharing of their information with law enforcement. This disclosure and consent is the foundation for ITAC's information sharing with law enforcement.

In 2005, ITAC signed a data sharing agreement with the U. S. Postal Inspection Service under which we provide, on a weekly basis, information about the victim and the circumstances of the identity theft incident. Over the past year, USPIS loaded information about the 6,000 ITAC cases into their Financial Crime Database which is used by postal inspectors all over the country. Also last year, we signed a data sharing agreement with Federal Trade Commission. Each week, we send the same data to the FTC which adds ITAC data to their Consumer Sentinel Database. As you know, 1,400 local, state and federal agencies have access to the Consumer Sentinel Database. We also work with the FBI and the Secret Service who have 24-hour-a-day online access to ITAC data via the FTC's database.

These are landmark agreements. In the past, many financial institutions shared information about their own identity theft cases with local, state and federal agencies. This one-on-one information sharing continues to this day and is very valuable. But ITAC's data sharing is unique because the information represents verified cases of identity theft from many different companies, it is national in scope and is delivered in a consistent format.

ITAC data gives law enforcement a 360-degree perspective. They can compare ITAC data to other information they have and determine the scope of the crime. Is there a single victim? Are there multiple victims? Is the perpetrator operating in the United States, or are they offshore? Are the crooks using the proceeds of their crimes

to buy a big screen TV, or to finance terrorism? ITAC data can help law enforcement answer these questions.

Our law enforcement partners report that data from ITAC is helping them catch and prosecute identity thieves. The U.S. Postal Inspection Service recently advised us that ITAC data has been used in more than a dozen cases where suspects have been identified, and in some cases arrested. For example, a recent case in Massachusetts involved four ITAC complaints and an estimated $167,000 in losses. False changes of addresses were used to divert mail containing financial documents belonging to five individuals. The information was used to order ATM cards and to make postal money order purchases.

With data sharing established at the federal level, we are moving to forge partnerships at the local and regional level where these cases are investigated and prosecuted. Just last week, ITAC signed a data sharing agreement with the Regional Identity Theft Network which was developed and is led by the US Attorney – EDPA. This innovative project include federal agencies (U. S. Postal Inspection Service, FBI, Secret Service, DHS and State Department), as well as the Pennsylvania Attorney General and District Attorneys in Philadelphia County and surrounding counties and offers a strategic solution to the size and information challenges mentioned above.

We also are moving forward with analysis of the ITAC data. With 6,000+ records, the ITAC database is reaching a "critical mass" where we can begin to map trends and patterns which we hope will help member companies detect and prevent identity theft. We will continue to identify new partners at the state and local law level. Finally, ITAC is inviting more companies – both in the financial services industry and in other industries including retailing and telecommunications – to join ITAC.

Mr. Chairman, I would be happy to answer any questions you may have.

Mr. COBLE. Thank you, Ms. Wallace.
Ms.——
Ms. MONTEZEMOLO. Montezemolo.
Mr. COBLE. Montezemolo.
Ms. MONTEZEMOLO. Happens all the time, sir.
Mr. COBLE. It's very rhythmic. It sounds very rhythmic.
Ms. MONTEZEMOLO. It's Italian. I'm proud of it. Thank you.
Mr. COBLE. You say it better than I do.
Ms. MONTEZEMOLO. I appreciate that.
Mr. COBLE. You are recognized.

STATEMENT OF SUSANNA MONTEZEMOLO, POLICY ANALYST, CONSUMERS UNION

Ms. MONTEZEMOLO. Well, good morning, Chairman Coble and Ranking Member Scott.

Thank you for the opportunity to testify on this important subject. I am also testifying today on behalf of the U.S. Public Interest Research Group.

Identity theft is a serious crime with over $55 billion in fraud each year. Studies show that the majority of victims don't know how their data were stolen, and there are plenty of victims, about 10 million each year who collectively spend 197 million hours working in that year to repair the damage done to their credit.

Worst of all for consumers is that even if they do everything right, like checking their credit reports and paying their bills on time, they can still become victims of ID theft through no fault of their own.

For example, last year, over 55 million Americans learned that their personal data had been compromised in preventable data breaches. It's hard to know how many have become victims of ID theft because thieves may sell stolen information to others or hold onto that information for future use or sale. But the FTC has documented at least 800 cases of identity theft arising from the ChoicePoint breach alone.

One question we ask when we consider Federal legislation is will this make consumers better off than they are today under State laws? We certainly hope that the Federal Government will help prevent identity theft before it occurs, provide consumers with tools to mitigate their risks based on the strongest State laws, and allow States to continue to innovate to protect our consumers.

But we are concerned that Congress will enact weak consumer protection and overturn State laws that are currently working very well. It is under this framework that we evaluate H.R. 5318, which requires notice to Federal law enforcement officials as identity fraud to Federal racketeering statutes and designates funding for criminal prosecution of ID theft.

The legislation does not address some of the broader consumer protection issues, such as, first, notifying individuals, not just the Federal Government, when their sensitive personal information has been compromised so that they can take steps to avoid or detect, at a much earlier time, identity theft.

Second, giving consumers the choice to lock their credit files so that identity thieves can't open new accounts in their names. This is known as a security freeze.

Third, letting consumers review and dispute the information held by largely unregulated companies like—called data brokers, like ChoicePoint.

Fourth, establishing security standards for companies that use our sensitive personal information. Several other Committees have passed legislation that covers these broader areas, and it seems possible that H.R. 5318, which deals with just the criminal justice piece of the puzzle, will be combined with broader legislation.

On its own, H.R. 5318 could complement State laws. But if it is combined with H.R. 3997, the Financial Services bill that Consumers Union, U.S. PIRG, and several other public interest groups strongly oppose, consumers would be worse off than they were prior to the ChoicePoint fiasco 15 months ago.

Let me give you some background on the Financial Services bill. It is completely one-sided. It guts existing State laws designed to give consumers the tools they need to prevent identity theft while putting in place very weak Federal standards.

For example, and most egregiously, it overturns the 17 State security freeze laws, including 11 laws that apply to all consumers. In its place, it limits a security freeze to victims of ID theft, which is too little, too late and means that the freeze can't be used as a prevention tool as it is intended.

H.R. 3997 also overturns State notice of breach laws, many of which ensure that individuals are notified whenever their unencrypted sensitive information has been compromised. Instead, it requires individual notification only after the company experiencing the breach decides that consumers are at risk of harm or inconvenience.

We call this the "don't know, don't tell" policy because if a consumer doesn't know whether consumers—sorry. Because if a company doesn't know whether consumers could be harmed, they don't have to notify them.

I could go on about the perils of this bill, but the point I am making is that H.R. 5318 should not be considered in a vacuum. It should be examined in the context of a broader Federal response.

If H.R. 5318 moves, we would much prefer that it be combined with H.R. 4127, the compromise identity theft bill that was unanimously reported out of the Energy and Commerce Committee. This bill avoids the "don't know, don't tell" approach to notification, leaves security freezes up to the States, and gives us all the right to review our data broker files and dispute any inaccuracies.

In sum, I urge you to tread carefully as you move forward in consideration of H.R. 5318.

Thank you, and I look forward to answering your questions.

[The prepared statement of Ms. Montezemolo follows:]

PREPARED STATEMENT OF SUSAN MONTEZEMOLO

Chairman Coble, Ranking Member Scott, and members of the subcommittee, thank you for the opportunity to testify on this important subject. I am also testifying today on behalf of the U.S. Public Interest Research Group.

Identity theft is a serious crime, with over $55 billion in fraud each year. Studies show that the majority of victims don't know how their data were stolen. And there are plenty of victims - about 10 million each year, who collectively spend 197 million hours a year working to repair the damage done to their credit.

Worst of all for consumers is that even if they do everything "right," like checking their credit reports and paying their bills on time, they can still become victims of ID theft through no fault of their own.

For example, last year, over 55 million Americans learned that their personal data had been compromised in preventable data breaches. It's hard to know how many have become victims of ID theft, because thieves may sell stolen information to others, or hold onto information for future use or sale. But the FTC has documented at least 800 cases of identity theft arising from the ChoicePoint breach alone.

One question we ask when we consider federal legislation is - "will this make consumers better off than they are today under state laws?"

We certainly hope that the federal government helps prevent identity theft before it occurs; provides consumers with tools to mitigate their risks, based on the strongest state laws; and allows states to continue to innovate to protect their consumers.

But we are concerned that Congress will enact weak consumer protections and overturn state laws that are currently working very well.

It is under this framework that we evaluate H.R. 5318, which requires notice to federal law enforcement officials, adds identity fraud to federal racketeering statutes, and designates funding for criminal prosecution of ID theft.

The legislation does not address some of the broader consumer protection issues, such as:

(1) First, notifying individuals when their sensitive information has been compromised, so they can take steps to avoid or detect at a much earlier time identity theft.

(2) Second, giving consumers the choice to lock their credit files so that identity thieves can't open new accounts in their names - known as a security freeze.

(3) Third, letting consumers review and dispute the information held by largely unregulated data brokers like ChoicePoint.

(4) Fourth, establishing security standards for companies that use our sensitive personal information.

Several other committees have passed legislation that covers these broader areas, and it seems possible that H.R. 5318, which deals with just the criminal justice piece of the puzzle, will be combined with broader legislation.

On its own, H.R. 5318 could complement state laws. But if it is combined with H.R. 3997, the Financial Services bill that Consumers Union, U.S. PIRG, and several other public interest groups strongly oppose, consumers would be worse off than they were prior to the ChoicePoint fiasco fifteen months ago.

Let me give you some background on the Financial Services bill. It is completely one-sided. It guts existing state laws designed to give consumers the tools they need to prevent identity theft, while putting in place very weak federal standards.

For example, and most egregiously, it overturns the 17 state security freeze laws, including the 11 laws that apply to all consumers. In its place, it limits the security freeze to victims of ID theft, which is too little, too late - and means that the freeze can't be used as a prevention tool.

H.R. 3997 also overturns state notice of breach laws, many of which ensure that individuals are notified whenever their unencrypted sensitive information has been compromised. Instead, it requires individual notification only after the company decides that consumers are at risk of harm or inconvenience. We call this "don't know, don't tell" because if a company doesn't know whether consumers could be harmed, they don't have to notify them.

I could go on about the perils of this bill - but the point I am making is that H.R. 5318 should not be considered in a vacuum. It should be examined in the context of a broader federal response.

If H.R. 5318 moves, we would much prefer that it be combined with H.R. 4127, the compromise identity theft bill that was unanimously reported out of the Energy and Commerce Committee. This bill avoids the "don't know don't tell" approach to notification, leaves security freezes up to the states, and gives us all the right to review our data broker files and dispute any inaccuracies.

In sum, I urge you to tread carefully as you move forward in consideration of H.R. 5318.

Thank you, and I look forward to answering your questions.

Consumers Union
Nonprofit Publisher of Consumer Reports

H.R. 5318 – Sensenbrenner "Cyber-Security Enhancement and Consumer Data Protection Act of 2006"

I. H.R. 5318 should be seen in broader context of House action.

H.R. 5318 is more limited in scope than many of the other data security bills that have been passed out of committee thus far, dealing with criminal penalties and notification to law enforcement officials in the event of a "major security breach" of more than 10,000 people.

Consumers Union (CU) has two concerns with this bill.

- First, we are concerned that the bill may be construed to preempt state individual notification laws, even though it does not address the issue of individual notification. This could occur if a court saw a conflict between state laws obliging notice to individuals unless law enforcement requests a delay and this federal bill which would require notice to federal law enforcement before any notice to individuals under state or federal law. We have proposed to both majority and minority staff the following technical change in language to clarify that the bill does not preempt state individual notification laws, adding a new paragraph to Sec. 7 (insert it right after the existing paragraph (c):

  "(d) The notice required by (a) shall be in addition to any other notice required under State or Federal law following the discovery of a security breach. Nothing herein shall be deemed to annul, alter, affect, or exempt any person from complying with the laws of any State with respect to notice of a security breach, except as provided by the specific requirements of (c)."

- Second, we are concerned that the bill, which is limited in scope, may be combined with another, broader vehicle. Currently, two such vehicles have passed tH.R.ough Committee in the House. These bills offer radically different results for consumers – the weak H.R. 3997, which has been reported out of the House Financial Services Committee, and the stronger H.R. 4127, which was unanimously reported out by the House Energy and Commerce.

CU joined with many other public interest groups in strongly opposing H.R. 3997, and we believe that consumers would be worse off if such a bill becomes law than if Congress takes no action at all. A much better outcome would be if the Sensenbrenner bill is attached to H.R. 4127, a bill supported by Consumers Union as a balanced and moderate approach to data security issues.

CU believes that H.R. 5318 must be considered in this broader context. The bill, if attached to H.R. 3997, could actually do much more harm than good. Below, we review the major issues under debate in the 109th Congress and summarize how H.R. 3997 and H.R. 4127 address them. After that, we include a list of bills under active consideration in the House and Senate, including the bipartisan bill coming out of the Senate Judiciary Committee, S. 1789, which was reported out of committee last year and is much more comprehensive than the Sensenbrenner bill.

II. Key issues in the federal debate and key differences between the two House vehicles (H.R. 3997 and H.R. 4127)

- **Notice of breach to individuals.** Individuals need to be notified when the security of their unsecured, sensitive personal information (e.g., Social Security number, date of birth, financial account number, etc.) has been breached, so that they can take reasonable steps to prevent becoming a victim of identity theft. In addition, when companies know they will have to notify individuals when data have been compromised, those companies have more of an incentive to take effective preventative steps to protect the data from being breached in the first place.

  H.R. 3997 requires notice only if the information whose security has been breached is "reasonably likely to be misused in a manner causing substantial harm or inconvenience to any consumer to whom the information relates." This is weaker than many state laws, which require notification whenever sensitive data have been breached. If a company does not know whether there is a risk of ID theft, then it does not have to notify. We call this the "don't know, don't tell" trigger.

  H.R. 4127 is also weaker than the strongest state laws, but it represents a better, and more consumer-friendly, compromise. It is drafted as an exception rather than a trigger. That is, under H.R. 4127, companies are required to notify unless they find that there is no reasonable risk of harm. When a company doesn't know whether there is harm, consumers are still notified.

- **Security freeze.** This is the most effective tool to prevent identity theft. In its strongest form, it allows each consumer the choice to "lock" his or her credit file against anyone trying to open up a new account or to get new credit in the name of the consumer. When a security freeze is in place, an identity theft can't open up a new account in the victim's name because the potential creditor or seller of services can't check the consumer's credit. A consumer may temporarily or permanently lift the freeze when he or she is applying for credit.

  Seventeen states have enacted security freeze laws, and eleven of those make the freeze available to all consumers. Two states that limit the freeze to ID theft victims only have passed and sent to the state Governor legislation to expand the freeze to all consumers. H.R. 4127 leaves the whole issue of security freezes to the states. H.R. 3997 eliminates state security freeze laws and replaces them with a very weak federal freeze that no one can access until after he or she has already been victimized by ID theft. This makes little sense, since the freeze is most effective to prevent becoming a victim of ID theft.

- **Access and correction of data broker files.** Data brokers like ChoicePoint collect and sell a wide range of information on all of us – including financial and biometric data, as well as arrest records, health, and employment records. They are unregulated, except to the extent that they are considered financial institutions under the Gramm-Leach-Bliley Act (GLBA) or are covered by the Fair Credit Reporting Act (FCRA). Because these institutions sell our most personal data to a wide range of clients, both public and private, it is critical that individuals be able to review this information and correct any inaccuracies. H.R. 3997 provides no right to see or dispute the contents of a data broker file. H.R. 4127 provides for both.

- **Information security safeguards.** GLBA requires that certain types of companies adopt appropriate physical, technical, and administrative safeguards on certain data. Many of the bills under consideration in the House and Senate would impose a requirement on all companies that hold specific types of data about individuals to have a security policy. Both H.R. 4127 and H.R. 3997 have this type of "safeguards" provision, but their effects on state laws are dramatically different. H.R. 4127 displaces only state laws that expressly require information security practices and treatment of data in electronic form similar to any of those required by the federal bill. H.R. 3997 displaces all state laws with "respect to the responsibilities, or the functional equivalents of such responsibilities" to "protect the security or confidentiality of information on consumers" and to "safeguard such information from potential misuse."

- **Preemption.** Preemption is an important issue in the debate over identity theft, since states have led the way in providing for breach notice, security freeze laws, and other innovations. Preemption of state notice of breach laws will be less important if Congress enacts strong standards and dual enforcement for notice of security breaches. However, identity thieves are fast-acting and fast-changing, and a federal ID theft law that extends broad preemption beyond notice could prevent states from keeping up with these criminals. Congress could do much more harm than good if it enacts weak federal standards while stopping existing and new state laws.

  H.R. 4127 preempts only state laws that require notification to individuals of a security breach and state laws that require information security practices similar to those in the bill. It leaves other issues for progress by the states. H.R. 3997 broadly preempts state laws that protect the security or confidentiality of information from potential misuse, require investigation or notice of any unauthorized access to information concerning consumers, require mitigation of any loss or harm from such access or misuse, or allow consumers to place security freezes on their credit files.

- **Enforcement.** A strong enforcement mechanism provides companies with an incentive to follow the law. At the very least, any Congressional bill should allow for enforcement by state attorneys general, to ensure that even if federal agencies don't have the will or the resources to go after bad actors, the law can be enforced. H.R. 4127 provides for this dual enforcement by state and federal government entities; H.R. 3997 does not.

III. Summary of ID theft bills under active consideration in House and Senate

H.R. 4127, the Data Accountability and Trust Act (DATA) – CU Supports

- Status: Passed House Energy & Commerce Committee.
- Lead sponsors: Representatives Stearns, Pryce of Ohio, Upton, Radanovich, Bass, Bono, Ferguson, and Blackburn.
- Notice: Individuals are notified of breaches of the security of certain personal information except where there is "no reasonable basis risk of identity theft, fraud, or other unlawful conduct."
- Security of sensitive information: Requires the FTC to establish rules for the security of personal information.

- Gives consumers free annual review of their data broker files and the right to dispute the contents of those files.
- Enforcement: Allows for enforcement by the FTC and by state AGs.
- Preemption: Displaces state laws, regulations, or rules that expressly require information security practices similar to those in the bill, and state laws that require notification to individuals of a security breach.
- Sunset: Expires ten years after the date of enactment.

H.R. 3997, Financial Data Protection Act – CU Opposes

- Status: Passed the House Financial Services Committee
- Lead sponsors: Representatives LaTourette, Hooley, Castle, Pryce of Ohio, and Moore of Kansas
- Scope: Applies to entities regulated by the Fair Credit Reporting Act (FCRA)
- Notice: Requires notice only if the information whose security has been breached is "reasonably likely to be misused in a manner causing substantial harm or inconvenience to any consumer to whom the information relates." The company deciding whether to give notice under this standard may consider whether security programs are likely to detect future fraudulent transactions.
- Security of sensitive information: Obligation to establish and maintain "reasonable policies" to protect the security and confidentiality of sensitive information against "unauthorized use that is reasonably likely to result in substantial harm or inconvenience." Compliance with the Gramm-Leach-Bliley Act, where applicable, complies with this Act.
- Security freeze: Provides security freeze for victims of ID theft only. Eliminates broader state security freeze laws.
- Enforcement: No state AG enforcement; enforcement only tH.Rough the functional federal regulator.
- Preemption: Preempts state laws to protect the security or confidentiality of information from potential misuse; state laws to investigate or provide notice of any unauthorized access to information concerning consumers; state laws to mitigate any loss or harm from such access or misuse, and state security freeze laws.

S. 1789, Personal Data Privacy and Security Act – CU Supports

- Status: Passed by the Senate Judiciary Committee; awaiting action by the full Senate.
- Lead sponsors: Senators Specter, Leahy, Feinstein, and Feingold.
- Notice of breach: Individuals are notified of security breaches by businesses and federal government entities unless the breached entity submits a risk assessment in writing to the U.S. Secret Service that finds that there is no significant risk of harm. Notice also is not required when the security of financial account information such as debit or credit card numbers is compromised if the business uses a security program designed to block unauthorized transactions before they are charged to the account. Makes knowingly covering up a breach a crime.
- Security of sensitive information: Establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personal information.

- Data brokers: Gives individuals the right to review their data broker file for a reasonable fee, as well as the right to dispute and correct inaccuracies.
- Enforcement: Provides for enforcement by state Attorneys General (AGs).
- Preemption: Displaces state laws related to notification of a security breach, except for additional victim protection assistance provided for by state law. Eliminates all state laws relating to individual access to and correction of personal electronic records held by data brokers. Generally does not preempt state laws requiring data security unless they are inconsistent with federal law.

S. 1408, Identity Theft Protection Act

- Status: Passed Senate Commerce Committee; awaiting action by the full Senate.
- Lead Sponsors: Senators Stevens, Smith, McCain, Inouye, Bill Nelson, and Pryor
- Notice of breach: Notice to individuals required only when there is a reasonable risk of identity theft.
- Security of sensitive information: Requires companies to develop, implement, maintain, and enforce a written program for the security of sensitive information.
- Security freeze: Allows all individuals to place a security freeze on their credit files for a reasonable fee set by the Federal Trade Commission (FTC).
- Social Security Number (SSN) restrictions: Prohibits the solicitation of the SSN if another identifier can reasonably be used. Prohibits display of SSN on employee or student identification card or tag. Bans sale of SSNs unless there is consent or certain other exceptions.
- Enforcement: Provides for enforcement by state AGs.
- Preemption: Displaces state laws on information security programs, notice of security breaches; state laws on solicitation or display of SSNs; and state-created liability for failure to notify of a security breach or to implement or maintain an adequate security program.

S. 1326, the "Notification of Risk to Personal Data Act" – CU Opposes

- Status: Passed Senate Judiciary Committee; awaiting action by full Senate.
- Lead Sponsor: Senator Sessions
- Notice of breach: Requires notice to individuals only "when there is a reasonable basis to conclude that a significant risk of identity theft to an individual exists." Includes a "safe harbor" provision shielding companies with existing notification policies which are consistent with the timing requirements of the Act from having to comply with other requirements of the Act including the contents of the notice and the manner of giving the notice.
- Security of sensitive information: Provides for the implementation of reasonable security standards to protect sensitive personal information from unauthorized access, destruction, use, modification, or disclosure.
- Enforcement: Allows for state AG enforcement.
- Preemption: Displaces state and local laws that relate "in any way" to electronic information security standards or individual notification of breach.

Contacts:
Susanna Montezemolo, 202.462.6262 ext. 1103, montsu@consumer.org
Gail Hillebrand, 415.431.6747 ext. 136, hillga@consumer.org

Mr. COBLE. Thank you.

And ladies and gentleman, we—Mr. Scott and I apply the 5-minute rule against us as well. So if you all could respond tersely, we could move along more respectively, I think.

Ms. Parsky, I am a victim. I am a cyber-crime victim. Whom do I call in the Federal Government?

Ms. PARSKY. Well, a lot of it depends on where you're located. There are a number of regional task forces across the country. Some are led by the local FBI field office. Some are led by the Secret Service. And so, it really is specific to your local community where your best resources are, but it is critical that you report to law enforcement right away.

And one of the things that we really appreciate about H.R. 5318 is a recognition of how important it is that companies and victims report to law enforcement. Unfortunately, we've seen a trend that even though these crimes are increasing and becoming more sophisticated, that the level of reporting to law enforcement has been decreasing.

Mr. COBLE. But it would be FBI or Secret Service?

Ms. PARSKY. Yes. And it would be really specific to the resources in the local community.

Mr. COBLE. Now the bill before us, Ms. Parsky, would amend the RICO statute to enhance law enforcement efforts to prosecute cyber-crimes. How does the Justice Department currently prosecute these crimes, and what role do States play? And how will the new RICO provision enhance the Justice Department's efforts and role?

Ms. PARSKY. Well, currently, the Justice Department uses a number of different statutes at its disposal. With respect to organized criminal syndicates that are now perpetrating cyber-crimes and identity theft crimes, we have used and will continue to use the general conspiracy statute, 3371.

But in addition, in recognition of the fact that this crime is becoming more sophisticated, that it's becoming a money-making operation, that other types of organized crime groups are latching onto it as a way to make money for their groups, we think that adding the serious felony provisions of 1030 would provide a very useful tool in addressing the way the crimes evolve.

Mr. COBLE. Thank you.

Mr. LaRocca, what new costs or expenses have the retail business community incurred in fending off cyber-criminals and/or investigating cyber-crimes?

Mr. LAROCCA. Mr. Chairman, while I cannot offer you a specific number because it crosses so many different retailers in so many different ways—and as I said earlier, many of these incidents go unreported—companies are forced to spend thousands or even millions of dollars on their technical infrastructure to set up firewalls and do security reviews of their system to identify potential acts of hacking or bots on their system.

This is in addition to the number of lost hours or costs associated with the restoration of their systems if one of these criminal attacks gets through. And for retailers in specific, the loss is associated with the theft of credit card information or identity information that's then used to make fraudulent purchases across the companies.

Mr. COBLE. Ms. Wallace, how does ITAC interact with Federal and State law enforcement to assist consumers? And do you have an established relationship with the FBI and the Secret Service?

Ms. WALLACE. Mr. Chairman, we interact with law enforcement at the Federal, State, and local level through the sharing of data from the ITAC victim assistance process.

We believe that that sharing is very valuable to consumers because it is going to result in deterrence of the criminals. That we are going to get more investigations, more prosecutions, more convictions, and that will deter the criminals.

We think that this deterrent effect is extremely important because consumers want to know that these crimes will be prosecuted, that there will be justice.

Mr. COBLE. Ms. Montezemolo, I'm going to get with you. We're going to probably have a second round. I'll get with you.

I want to put this question, Ms. Parsky, primarily to you, or to anyone. I am thoroughly convinced that organized crime is joined at the hip with terrorism. Illegal drug trafficking joined at the hip with terrorism.

What evidence do you all have, if any, that the cyber-criminals are connected either directly or indirectly with terrorism? Any evidence to that end?

Ms. PARSKY. Well, Mr. Chairman, I agree with you, and we see this across the board that wherever you have a type of criminal activity that's latched onto by organized crime groups to make money, that there is a very strong potential for that also to be used by terrorist organizations. And we see that across the board.

We've also seen that the use of the Internet and the use of computers to facilitate terrorist activity has been an issue and has been evidenced in a number of the prosecutions that we've brought.

Mr. COBLE. I thank you, and my red light appears.

Before I recognize the distinguished gentleman from Virginia, I want to welcome the distinguished gentleman from California, Mr. Lungren, for having joined us.

And now I'm pleased to recognize Mr. Scott.

Mr. SCOTT. Thank you.

Mr. LaRocca, you indicated that many of these crimes go unreported. Is that because you don't think they're going to be prosecuted?

Mr. LAROCCA. In some cases, it could be that they will not be prosecuted. In others, it could simply be that the company may face public scrutiny or embarrassment in the media. And if this was a publicly held company, that obviously has, you know, great concerns and could have impact on its share and its stockholders.

Mr. SCOTT. Thank you.

Ms. Wallace, there were about 8 million incidences of identity theft last year. In each of those cases, listening to your testimony, it seems to me that you believe most of them could be solved if you did the investigatory work. Is that your belief?

Ms. WALLACE. Well, Mr. Chairman, I do think that many more cases of identity theft could be investigated and prosecuted, yes.

Mr. SCOTT. Things like a change, unauthorized change of address, are those ever prosecuted?

Ms. WALLACE. Well, that in itself may involve mail fraud, which may be a crime that the Postal Inspection Service could take a look at.

Mr. SCOTT. But I mean in the run of the mill case where somebody has got an identity theft scheme going on, part of which is a change of address that would let you know where the criminal is. Are those ever investigated?

Ms. WALLACE. You've really put your finger, Mr. Scott, on one of the key problems that law enforcement faces in this area, which is that the facts are so different and the jurisdiction is so different. And who has the best possible—you know, which agency has the best way of investigating that case varies so much.

Sometimes the best agency to investigate is Postal Inspection Service. Sometimes it's the State. So that kind of confusion and patchwork quilt sometimes really frustrates the investigations.

Mr. SCOTT. Well, these I imagine are somewhat labor intensive because you get—somebody gets an unauthorized charge on his credit card, and you report it, it takes some work. The—as I understand the traditional way of dealing with it is you cut off the card, you write off the illegal charges, and the victim is made whole.

The card is cut off, and the bank writes off the loss, and that's the end of it. It seemed to me if you let the card run, you could catch the person. Is that ever done, to your knowledge?

Ms. WALLACE. Well, Mr. Scott, I think that's something that you'd probably have to raise with the local investigators. We don't do the investigations ourselves. Our mission is to help the victim recover from that dreadful event.

Mr. SCOTT. Okay. But you have followed through, and with your database, you've been able to ascertain how these crimes have been occurring?

Ms. WALLACE. We are just getting to the point where we feel that we have enough data to start mapping trends and to show that, work with the law enforcement on that.

Mr. SCOTT. Now some of these are wholesale organized crime-sized operations. I imagine some of it is individuals just stealing somebody's card or buying a little information. Not an ongoing operation, but just one where they're just stealing a couple of thousand dollars.

So long as they think they can get away with it, that information is valuable. When they don't think they are going to get away with it, that information isn't as valuable. Isn't that the case?

Ms. WALLACE. The information is very valuable. And if I may——

Mr. SCOTT. Because if you steal it, you can run up a credit card a couple of thousand dollars and get away with it.

Ms. WALLACE. Information is the key to the value these days, yes, sir.

Mr. SCOTT. Well, and the fact that you're not going to get prosecuted.

Ms. WALLACE. It has not gone unnoticed by these criminals that many of them get away with it.

Mr. SCOTT. Ms. Parsky, my time is just about up. I'm interested in the task force. And because it sounds like your task force is deal-

ing with these questions I've just asked, but my time is about to run—I'm sorry?

Mr. COBLE. The President's task force.

Mr. SCOTT. The President's task force. And so, let me defer—my time is just about up. Let me defer, but that would be the question that I'd like Ms. Parsky to address.

Mr. COBLE. You may respond, Ms. Parsky. We'll suspend for the moment, and we will have a second round. Mr. Scott can start with that question.

We're pleased to have been joined with the distinguished gentleman from Florida, Mr. Feeney. And now the Chair recognizes the distinguished gentleman from California, Mr. Lungren, for 5 minutes.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

I'm particularly interested in this subject since I chair the Subcommittee that has responsibility for cyber-security in the Homeland Security Committee. And one of the concerns I have is that we are approaching this problem not exclusively, but significantly from the standpoint of after a crime has been committed and the kind of deterrence necessary to hopefully forestall that, but the ability to catch criminals and prosecute them.

And while that's all important, one of the concerns I've got is the lack of knowledge that we have among the consumers as to what they ought to do, what they can do, what they should do in terms of protecting themselves. And I am one of those consumers.

And let me—I'll start on the right and go all the way down, my right to left, and ask you, where are we on that? What can we do from the standpoint of the organizations you represent to have consumers be involved in self-help?

What can we do to raise the level of knowledge among consumers as to how vulnerable they are from identity theft so that their only reaction is not to get mad at their bank or their credit card company at the time that they find that somebody has already committed a crime against them?

And is there anything that we can do, well, at whatever level, to attempt to try and not only provide that information, but somehow provide incentives for consumers to pay attention to it? So that, in fact, number one, they protect themselves and, number two, if there is either an attempted theft or an actual theft, that they know how to respond in the quickest fashion, and that information gets involved in whatever mechanism we set up for ferreting this out and prosecuting these people.

Ms. MONTEZEMOLO. That's a great question, and I would begin by saying that even when consumers are doing everything that we at consumer organizations tell them to do—checking their credit report annually, each year, from each of the credit reporting agencies, checking their statements very carefully, perhaps placing a freeze if they live in a State that allows a freeze—they are still becoming victims of identity theft.

So even when consumers are doing everything right, they're still finding that they become victims of identity theft. So it's a very frustrating system.

I think one of the areas where consumers are best served actually is one where your State has been a leader, and that is in terms

of notification to the individual when a breach of their sensitive personal information, say, their Social Security number, has occurred.

So when that has happened—for example, with ChoicePoint last year and actually with over 100 other companies—when consumers are informed that they are at increased risk for identity theft, they can actually take steps to mitigate that risk and prevent becoming a victim.

For example, in California, they can place a security freeze on their credit file, which quite literally locks their credit file so that identity thieves can't open up new credit accounts in their name.

Mr. LUNGREN. What about Mr. Scott's concern—I don't know if I would say "concern." But the question he asked that if we do that immediately, you don't get a chance to catch the guy, catch the crooks.

It seems to me that that decision ought to be made by the consumer. That is, law enforcement contact them and let them know that that's happened. And then if they want to try and catch them, they would do that. But anyway, go ahead.

Ms. MONTEZEMOLO. Yes, I don't actually think that that is in conflict with what Mr. Scott was saying.

If you have a credit freeze, it doesn't prevent the thief from applying for credit in your name. They still go through and do that. What it stops is the thief from actually getting the credit in your name and running up all these charges. So we would still have the paper trail that said this person tried to apply for credit in your name.

And on top of that, I, as the consumer, the legitimate person, would get a call from the credit reporting agency that told me someone applied for a new credit card in your name. You know, you need to be more careful. And I might go to the police and be able to start that process.

Mr. LUNGREN. So requiring timely notice to the individual whose identity has been stolen is one of the——

Ms. MONTEZEMOLO. Or whose data has been breached so they're at increased risk for identity theft.

Mr. LUNGREN. Ms. Wallace?

Ms. WALLACE. Yes, Mr. Lungren. Let me respond to your question about consumer education and what more could be done to help consumers.

The Federal Trade Commission has done a fabulous job so far on publishing information. They have a terrific Web site, which is very helpful to consumers, as I'm sure the consumer organizations refer their consumers to the FTC's Web site, too.

And just yesterday, the FTC rolled a new identity theft consumer toolkit at the White House in conjunction with the President's signing of an executive order.

Mr. LUNGREN. See, I didn't even know that.

Ms. WALLACE. Oh, well.

Mr. LUNGREN. I mean, I'm reasonably—I pay attention to the news. I watch television. I occasionally listen to the radio and read the newspapers and try to keep up on that and——

Ms. WALLACE. Well, I'm happy to tell you about it because it's a wonderful program. And we in the financial services industry in-

tend to work with the FTC and are working with the FTC to actually push out this information to consumers. Our companies have been—in fact, we have a conference call this afternoon to push out this information to our companies so that they will be educated——

Mr. LUNGREN. Let me just ask it this way, and I know my time's up. But are we satisfied with consumers protecting themselves right now?

Ms. WALLACE. No, there's still more to be done.

Mr. LUNGREN. Is there any—can you quantify it? I mean, are we 20 percent there? Are we 50 percent there?

I mean, I'm concerned about this because, you know, you talk with most people, frankly, they don't know what their vulnerability is. They don't know what steps they should take. They don't know how often they ought to upgrade their systems.

And I believe in law enforcement. I've been in law enforcement a long time. But I also believe in the individual taking some responsibility for himself or herself. And are we giving them that information? Are we prodding them in ways that they can protect themselves?

Ms. WALLACE. There is growing consumer awareness, Mr. Lungren. The challenge is it is an ongoing consumer education issue.

Mr. LUNGREN. Right.

Ms. WALLACE. Because the thieves are endlessly inventive. And the challenges are always changing, and their methods are always changing. So it's a continuous process. You can never let up your guard.

Mr. COBLE. The gentleman by his own admission, by his own admission, did not know that. I thought Californians knew everything, Mr. Lungren. I've learned something today.

Mr. LUNGREN. Well, humility is found in strange places, Mr. Chairman.

Mr. COBLE. We will start a second round now.

Ms. Montezemolo, you note in your testimony that you have only one technical concern with the bill before us. If that issue is resolved in a manner that Consumers Union approves, will you generously embrace the bill?

Ms. MONTEZEMOLO. Well, I also want to just acknowledge that both your staff and the minority staff have been very generous in meeting with us and working on that issue, and that that issue is that we believe that the way the legislation is written, it may unintended—without being intended, preempt State security notification laws to individuals.

This is not something that the bill covers. So, in talking to your staff, we believe that that's unintended, and we appreciate that. And I think that, yes, we see this as a positive step forward dealing with the criminal side, and where our concerns lie are on the broader picture.

Mr. COBLE. Well, you've just touched on a point, and I think I'm guilty of omission. We are, indeed, richly blessed with good staff on both sides, majority and minority, and I don't extend them the due praise they're entitled to. So thank you for opening that door.

Mr. LaRocca, as it relates to loss prevention, does the retail business community—I'll ask the same question I put to Ms. Wallace.

Do you all have an established relationship with the FBI and the Secret Service?

Mr. LAROCCA. Mr. Chairman, we certainly do. Retailers really choose which agency to file a criminal complaint with based on where their field office is located or who they may have relationships with in that particular agency.

In other cases, the local jurisdictions will forward the case to the Federal authorities, and then jointly and collaboratively, the retailers will work with the Federal agencies in investigating and resolving the matter. As we see it, whoever gives us the best customer service by those agencies is who we'll file the report with.

Mr. COBLE. I got you.

The distinguished gentleman from Virginia?

Mr. SCOTT. Thank you, Mr. Chairman.

Ms. Parsky, the last time we were on this subject in March of 2004, a Mr. Coleman was testifying on behalf of the Department of Justice and was asked about my little bill, which would authorize $100 million to combat identity theft. And the Chairman asked given the fact that identity theft is intertwined with so many other crimes, how do you envision that these funds would be utilized to address the problem, and did the President request funds?

And his response in part was, we believe 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, Criminal Division, and working with regulatory offices. So they had enough resources.

Of course, later on in the hearing, when I asked him if they prosecuted small amounts of cases, his answer was, "There are resource constraints that cause U.S. attorneys' offices—that cause U.S. attorneys' offices to turn away cases that are not above a certain limit." And of course, I responded that my bill would address that problem.

It appears that your task force is dealing—looks like from the description, that you're dealing specifically with the problem of prosecuting these cases so that people won't run around thinking that if they can get somebody's credit card, they can go ahead and use it, and whatever they can get out of it, they won't be caught.

Will the task force address this perception?

Ms. PARSKY. The purpose of the task force is to marshal all of the Federal resources across the U.S. Government to really crack down on this problem. There are ongoing efforts in a number of different agencies in terms of education, in terms of prosecution and investigation at Department of Justice, Social Security Administration, the FTC. There are many organizations involved in trying to address the problem.

What the task force is looking to do is to really focus everyone's efforts, coordinate the efforts so that we not only increase prosecutions and investigations, but we also coordinate the type of public education that Congressman Lungren was talking about.

We coordinate better with our State and local partners, recognizing that this is a pervasive problem. That there are many ways that the Federal Government can address it, but there also are

really important ways that State and local law enforcement can work with us to address the problem.

Mr. SCOTT. Well, some of the—somebody's got to do the work. These are labor-intensive investigations. I was just jotting down some of the things that would take some time.

If you've got somebody's—if you know somebody's credit card has been stolen, if they go to the electronics store to buy one of these flat-screen TVs, they get the authorization for the charge. And while they're standing there waiting for the television, it looks like somebody could go there and catch them right there. But that takes time.

When somebody is using a—for just to get gasoline. Somebody can go to the gas station, if they have one those video cameras, and get a picture of the license plate. That takes—that takes time.

If there's a change of address, you can go to the new address, see who happens to be there. You might get some good information. You can notice, if you've got the information that Ms. Wallace is developing, you can find out that a lot of these things are going to the same address. That would be information, but that takes time.

Other times, you can find out where they went to use a card. A lot of these people have video cameras. You can see who did the charge. You can find that one guy who is doing some of this, you might be able to squeeze them in your traditional investigatory techniques, find out where did they get the card from and kind of work up if there's somebody.

I mean, this takes time and money to run these kinds of investigations. And my question is, do you have enough money to perform all of this labor-intensive investigation?

Ms. PARSKY. Well, I think, obviously, we always are looking for ways to work efficiently within the resources we have to be as effective as possible. I've been advised that in the Administration's '07 budget, there is a request for additional resources for identity theft prosecution.

Mr. SCOTT. How much?

Ms. PARSKY. I believe it's 30 more positions, 24 of which are attorneys, which brings the total identity theft budget to $18.7 million.

Mr. SCOTT. And they will do the low-level investigation or coordinate some of the low-level investigations so that people who are doing this can assume that they're going to get caught?

Ms. PARSKY. Well, I think what we're looking to do is—is find the most strategic ways to work with our partners so that we can not only find ways to address the individual violations, but also find ways to connect the dots.

And particularly in areas of cyber-crime, where the harm can be spread throughout the country, throughout the world, you know, it's important that we have those types of partnerships so that we can see the patterns and try to recognize when there are criminal organizations that are actually responsible.

Mr. SCOTT. Now is the FBI an appropriate place to put our resources, or should some of this be in grants to local law enforcement?

Ms. PARSKY. I think that obviously that the problem is large enough that we need to draw on all of our law enforcement resources to address it.

Mr. SCOTT. Some of this is interstate, so the local law enforcement would be somewhat hamstrung if somebody is doing a Statewide——

Ms. PARSKY. Correct.

Mr. SCOTT. Or FBI maybe. But you would need possibly some law enforcement, local law enforcement assistance. Would grants be helpful from that point of view?

Ms. PARSKY. That's something that obviously the part of the Justice Department that deals with those programs would be able to answer better.

Mr. SCOTT. Mr. Chairman, could I ask one other question?

Mr. COBLE. Without objection.

Mr. SCOTT. Ms. Montezemolo, if somebody is caught up in an identity theft problem—Ms. Wallace might also want to address this—can you get a new credit—can you get a new Social Security number and start from scratch? Transfer all of your Social Security information to the new number and just start from scratch? Is that possible?

Or are you stuck with the same Social Security number that the crooks will always have?

Ms. MONTEZEMOLO. It is extremely, extremely rare to be able to get a new Social Security number. It is technically possible, but it is very, very difficult to do.

And as a result of that, the Social Security number has become like the master key into our financial lives. And when a criminal has that along with, say, our date of birth, they can open up new accounts in our name. And not just today, but in the future. They could do that 10 years from now because that number is so unlikely to change.

Mr. SCOTT. Ms. Wallace?

Ms. WALLACE. Actually, thank you, Mr. Scott.

This gives me an opportunity to mention an initiative that the financial services industry is very interested in and is working with the Social Security Administration to set up a verification program, where financial services companies could actually ping against the Social Security database.

So that if we received an application that involved a Social Security number that seemed questionable, the creditor could at that point verify that it was a legitimate Social Security number. We think this is a—it's just in the organization stage. But we think this has great promise.

Mr. SCOTT. But if somebody has stolen my Social Security number——

Ms. WALLACE. This may prevent that Social Security number from being used again by the crook.

Mr. SCOTT. How?

Ms. WALLACE. If your Social Security number has been compromised, what that person may well do is try to open accounts or obtain other things of value. In applying for credit, the creditor could access the Social Security Administration database to verify

that that was a valid Social Security number or that, you know, there might be fraud involved.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. COBLE. The distinguished gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

Ms. Parsky, in your written statement, you say the FBI has made cyber-crime, including fraud, hacking, child pornography, and intellectual property crime on the Internet, one of its top three enforcement priorities. And you've spoken about how the Justice Department has increased their cyber-crime expertise.

We're talking here about identity theft, which is one part of it. Where does that fit in the scheme of things? Child pornography, intellectual property crime—where does identity theft fit?

And the reason I ask that is we can pass this legislation and we can have a few more people involved in cyber-crime, but what is the impact going to be versus the array of potential crime that is out there?

Ms. PARSKY. Well, certainly identity theft crosses over both the cyber-world and the physical world. And so, there are fraud-based units at the bureau and in the Justice Department that focus on these crimes as they are committed in the physical world. And we also have cyber-experts who focus on the crimes as they are committed in the cyber-world.

And certainly, a lot of the computer hacking, a lot of the cyber-crimes that we're seeing are being exploited for purposes of financial gain, which is often through identity theft, where you're stealing personal information from other computer systems in order to use that information for illicit gain, whether it's taking credit card information or bank account numbers and then using that for fraudulent purposes or other means.

So it's—what we're doing is really trying to address the problem in both the cyber and the physical context.

Mr. LUNGREN. Mr. LaRocca, if I'm a local prosecutor, local law enforcement officer, and I have a problem of child pornography on the one hand and identity theft on the other, I only have resources to investigate and prosecute one, 9 times out of 10, I'm probably going to go after child pornography.

We have limited resources. Local jurisdictions naturally concentrate on violent crime because that's what does the greatest damage to people as we see it. And so, my concern is and my question to you is, are you satisfied with the level of cooperation between local, State, and Federal authorities in the area of identity theft from your perspective?

If not, are there some recommendations you might make with this bill or in other areas that would improve that?

Mr. LAROCCA. Mr. Lungren, while identity theft and how it's investigated by law enforcement is not my expertise, from the relationship standpoint, I can tell you that we have seen a greater level of communication and collaboration between local, State, and Federal law enforcement agencies.

As a former Californian, I worked closely with a number of those groups while in the L.A. area. And of course, child pornography

would be a priority above identity theft. Our kids are our greatest asset.

However, this is an important issue, and I think it's not only the collaboration between the public sector, but it's also what we can do in the private sector as well. And to the questions that came up earlier, I think part of that is we can assist consumers and, you know, communicating and putting awareness campaigns out there.

And I think the other part that 5318 does is it stiffens the penalties, which may be a prevention for these would-be hackers that do it for fun or do it simply for the challenge. It puts some deeper risk with that gain that they're getting.

Mr. LUNGREN. Ms. Wallace, here's a concern I have. Obviously, I don't want to underplay identity theft. It's an extremely serious problem, and it's something that we have to deal with. But after we hear all the panelists talk, it is this exploding problem that continues, that sort of is like a cancer. It metastasizes at a rate that seems to outstrip our resources in the sense of us trying to keep up with it.

And so, again, I go back to the question of hitting it on the front end. And are there things that we can do which, in addition to us protecting ourselves, give law enforcement a quicker jump on the problem?

That is, the cooperation of the companies involved, the cooperation of consumers involved. And with respect to the companies involved, ought that to be mandated?

Ms. WALLACE. Mr. Lungren, with your permission, I'd like to come back to you with some specific recommendations on that topic. We are just beginning to work with these partners, and I think if we gave some consideration to it and talked to our members, we could give you some useful recommendations.

Mr. LUNGREN. Mr. Chairman, I guess my time is up.

Mr. COBLE. The distinguished gentlelady from California, Ms. Waters.

Ms. WATERS. Thank you very much, Mr. Chairman.

I am—I'm interested in a couple of issues that have been, I think, identified by the representatives of Consumer Unions, and that is preemption and notice of breach to individuals.

But without raising questions, it's obvious to me that this House is all over the place on these issues. And between the three Committees which have some jurisdiction in this area, it seems as if we are—we are in conflict on these two main issues that I'm concerned about.

So, you know, rather than even burdening the witnesses here with questions today, it seems as if the House needs to get its act together and not have, you know, three or four different bills floating around here that are in conflict with each other. And I will be paying special attention to, of course, preemption and the notice of breach to individuals.

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

Mr. COBLE. I thank the gentlelady.

The distinguished gentleman from Ohio, Mr. Chabot?

Mr. CHABOT. I have no questions, Mr. Chairman. Thank you for holding the hearing.

Mr. COBLE. Thank you, sir.

The distinguished lady from Texas, the gentlelady, Ms. Jackson Lee?

Ms. JACKSON LEE. I thank the witnesses for their testimony.

Mr. COBLE. Does the gentlelady yield back?

Ms. JACKSON LEE. I yield back at this time. Is there another questioner?

Mr. COBLE. Pardon?

Ms. JACKSON LEE. Is there another person to question?

Mr. COBLE. No.

Ms. JACKSON LEE. I yield back.

Mr. COBLE. Let me thank the witnesses for your testimony today.

Bobby? Do you have anything else, Bobby?

We appreciate this, and let me conclude this hearing, and then we'll go into a markup.

In order to ensure a full record and adequate consideration of this important issue, the record will be left open for additional submissions for 7 days. Any written questions, furthermore, that a member wants to submit to you all shall also be required to submit that inquiry within a 7-day timeframe.

This concludes the legislative hearing on H.R. 5318, the Cyber-Security Enhancement and Consumer Data Protection.

We appreciate your attendance for those in the hearing room, as well as the witnesses.

And the Subcommittee stands adjourned.

[Whereupon, at 10:15 a.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

PREPARED STATEMENT OF THE BUSINESS SOFTWARE ALLIANCE

BSA®
BUSINESS SOFTWARE ALLIANCE

1150 18th Street, NW
Suite 700
Washington, DC 20036

p. 202/872-5500
f. 202/872-5501

Written Statement

of

The Business Software Alliance

before the

House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security

on

H.R. 5318, the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006"

Mr. Chairman, Ranking Member Scott and other distinguished Committee members, the Business Software Alliance (BSA[1]) and its member companies thank you for this opportunity to provide a written statement commenting on H.R. 5318, the *"Cyber-Security Enhancement and Consumer Data Protection Act of 2006."* The Business Software Alliance is an association of the world's leading software companies and their key hardware partners. BSA's members create approximately 90% of the office productivity software in use in the U.S. and around the world.

BSA has stressed for several years the importance of maintaining confidence in the Internet and ecommerce. Unfortunately, online confidence is being threatened by increasingly sophisticated and organized criminal elements who are taking advantage of blind spots in current criminal statutes relating to cyber crime. Therefore, BSA strongly supports the provisions of this legislation that fill these gaps in the criminal code and give law enforcement the tools necessary to effectively find and prosecute cyber criminals.

[1] The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Dell, Entrust, HP, IBM, Intel, Internet Security Systems, McAfee, Microsoft, PTC, RSA Security, SAP, SolidWorks, Sybase, Symantec, Synopsys, The MathWorks, and UGS.

Under the legislation, law enforcement also would be notified of major security breaches where unauthorized access to sensitive personal information presents a significant risk of identity theft. BSA appreciates how early notification to law enforcement in certain circumstances could be helpful in preventing and minimizing potential harm. Although we have some concerns with the language of Section 7 as introduced, we look forward to working with the Committee to develop language that meets our shared goals.

GIVING U.S. LAW ENFORCEMENT OFFICIALS THE TOOLS NECESSARY TO FIND AND PROSECUTE CYBER CRIMINALS

Criminalizing malicious botnet attacks:
Section 2 would specifically criminalize the creation of Botnets. Increasingly, individuals who perpetuate harm through the use of computers do so by accessing and controlling protected computers remotely and without authorization. The compromised computers thus become "botnets" – a "robot network" of compromised "zombie" computers remotely controlled by an attacker. Botnets represent a significant danger because the people who control Botnets, often referred to as "Bot Herders," can build Botnets that involve several hundred thousand machines. These machines can be used to attack other machines, spread spyware, or disrupt Internet functions. BSA applauds the priority that the Department of Justice has given to cases involving "Bot Herders", as reflected prosecutions earlier this year of defendants in California and Washington. In the case in Seattle, for example, the defendant's botnet attack last year that caused the system at Seattle's Northwest Hospital to malfunction. These are extremely serious cases and we are pleased that the Justice Department recognizes the significant threats posed to the public by botnet attacks.

While BSA is grateful for the enforcement efforts by the Justice Department, we agree with the Committee that current law to support prosecutions of Bot Herders prior to an attack can be strengthened. Generally, current law is not well-tailored to support prosecution of Bot Herders. Even when a Botnet is large, it may be difficult for prosecutors to prove the damage necessary for a prosecution under current 18 USC Sec. 1030(a)(5). In addition, prosecutors may be reluctant to charge the creator of a Botnet under

the current section 1030(a)(2), because it may be difficult to prove that the Bot Herder "obtained information" from one of the attacked zombie computers.

Identifying, stopping, and prosecuting Bot Herders is critical for all users, including both consumers and critical infrastructures. Discovering and shutting down a Botnet is tantamount to identifying the precursors to and preventing identity theft, network disruption, and loss of intellectual property.

Botnets can result in widespread damage and deserve immediate attention. Cyber criminals are commoditizing Botnets and selling them to other would-be attackers. Trafficking of these attack tools can fund any number of other illegal activities. Additionally, the methodologies for assembling, and controlling Botnets are becoming increasingly sophisticated and difficult to trace.

We are grateful that the Committee has proposed language that would amend18 USC Sec.1030(a)(2) and thus, will help reduce this serious and growing threat. The legislation clarifies that the law prohibits the type of malicious activity that is associated with botnets.

Closing loopholes in law enforcement's ability to prosecute unlawful activity:
Today, 18 USC Sec.1030 only guards against unauthorized access to a computer which is used in interstate or foreign commerce or communications and the cyber criminal's conduct in obtaining information from such a computer itself involved an interstate or foreign communication. Section 3 of this bill provides that a protected computer also is one which affects interstate commerce and that it is illegal to obtain information from any protected computer without authorization.

Covering cyber racketeering through the addition of RICO predicates:
BSA feels that Section 4 of H.R. 5318 correctly updates RICO predicate offenses to give U.S. law enforcement the legal ability to effectively investigate and prosecute organized crime syndicates.

Organized crime syndicates from Eastern Europe, Africa, Asia and other regions have been identified as significant culprits behind phishing scams, identity theft, online extortion and other cyber crime activities. However, until now, no action has been taken to update

the predicate offenses to support a racketeering criminal charge. This bill fixes that problem by including these underlying offenses.

Covering cyber extortion:
BSA appreciates that H.R. 5318 seeks to prohibit cyber extortion where the criminal threatens to access a protected computer and demand a non-monetary promise or agreement from the victim.

Existing definitions of extortion in 18 U.S.C. §§ 875 and 1030 criminalize threats communicated with the intent to extort "money or other thing of value." Some threats, which may be terrifying and damaging, do not demand "things," but instead demand that the recipient refrain from lawful conduct or suffer denial of service attacks, posting of confidential information online, and identity theft. The threats do not demand either money or things of value.

While cyber criminals often threaten online businesses with cyber-attacks for the purposes of extorting money, cyber extorters often harass and attack without explicit demands for things of value. Rather some extorters may seek to cripple a competitor's online services or carry through on a vendetta. Spamhaus.org an international non-profit organization whose stated mission is "to track the Internet's Spam Gangs, to work with Law Enforcement Agencies to identify and pursue spammers worldwide." They and a number of high profile anti-spam organizations have been the frequent target of denial-of-service attacks (the most common cyber extortion tool) from the combined efforts of spammers, hackers, and virus writers. The spammers did not attack to extort money, but rather wished to cripple organizations and services that had blacklisted them.

Updating criminal statues to address this type of cyber extortion is vital to the protection of law-abiding citizens. We look forward to working with Committee to refine the language of Section 5 to clearly address these needs.

Including conspiracy to commit cyber crime:
BSA supports Section 6 of the bill which seeks to target the growth of the organized crime element in cyber crime. As organized crime becomes more involved in cyber crime, focusing the penalty structure on illegal group behavior becomes more important. Adding an explicit conspiracy charge to § 1030, rather than relying upon the general criminal conspiracy statute in 18 U.S.C. § 371, would not only subject conspiracy recidivists to enhanced penalties under § 1030 but also treat conspiracies to commit such offenses similarly to attempts, which are arguably less egregious than illegal group activity and are explicitly criminalized in this statute.

Forfeiting property used to commit cyber crime:
BSA supports the bill's provision under Section 8 which requires cyber criminals to forfeit to the US any real or personal property that is used or intended to be used to commit or to facilitate the commission of a computer crime

Property, both real and personal, that is derived from proceeds traceable to a violation of 18 U.S.C. § 1030 is currently subject to both criminal and civil forfeiture. We agree that forfeiture should include computers, equipment, and other personal property used to violate the CFAA, as well as real and personal property derived from the proceeds of computer crime.

Expanding sentencing guidelines:
Currently, sentences for violations of 18 U.S.C. § 1030 are determined by calculating actual economic loss, which is often difficult to determine in the computer crime context. Defendants convicted of computer crimes often serve no term of imprisonment, resulting in the absence of any deterrent effect arising from criminal prosecution and making computer crimes less likely to be prosecuted in the future.
Section 9 of the bill directs the US Sentencing Commission, in determining its guidance on the appropriate sentence for computer crime, to consider a number of highly relevant factors in order to create an effective deterrent to computer crime.

Increasing funding for law enforcement to fight cyber crime: BSA strongly supports Section 10 of the bill. The need for more dedicated law enforcement personnel and advanced forensic tools to investigate and assist in the prosecution of computer crimes is greater than ever. It is essential that law enforcement has the resources necessary to hire and train additional law enforcement officers dedicated to investigating crimes committed through the use of computers and other information technology, including through use of the Internet, and for the procurement of advanced tools of forensic science to investigate and study such crimes.

NOTIFYING LAW ENFORCEMENT OF MAJOR SECURITY BREACHES

Under the legislation, law enforcement also would be notified of major security breaches where unauthorized access to sensitive personal information presents a significant risk of identity theft. BSA appreciates how early notification to law enforcement in certain circumstances could be helpful in preventing and minimizing potential harm.

We do, however, believe there are changes to the language of Section 7, as introduced, that would focus law enforcement's attention and actions on the truly significant cases and would not impose undue burdens on victims of cyber crime. We look forward to working with the Committee as the process moves forward.