AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 110–62

IDENTITY THEFT: INNOVATIVE SOLUTIONS FOR AN EVOLVING PROBLEM

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MARCH 21, 2007

Serial No. J–110–22

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

35–797 PDF WASHINGTON : 2007

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

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ARLEN SPECTER, Pennsylvania
JOSEPH R. BIDEN, JR., Delaware	ORRIN G. HATCH, Utah
HERB KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	JON KYL, Arizona
RUSSELL D. FEINGOLD, Wisconsin	JEFF SESSIONS, Alabama
CHARLES E. SCHUMER, New York	LINDSEY O. GRAHAM, South Carolina
RICHARD J. DURBIN, Illinois	JOHN CORNYN, Texas
BENJAMIN L. CARDIN, Maryland	SAM BROWNBACK, Kansas
SHELDON WHITEHOUSE, Rhode Island	TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MICHAEL O'NEILL, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

DIANNE FEINSTEIN, California, *Chairman*

EDWARD M. KENNEDY, Massachusetts	JON KYL, Arizona
JOSEPH R. BIDEN, JR., Delaware	ORRIN G. HATCH, Utah
HERB KOHL, Wisconsin	JEFF SESSIONS, Alabama
CHARLES E. SCHUMER, New York	JOHN CORNYN, Texas
RICHARD J. DURBIN, Illinois	SAM BROWNBACK, Kansas
BENJAMIN L. CARDIN, Maryland	TOM COBURN, Oklahoma

JENNIFER DUCK, *Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	1
Kennedy, Hon. Edward M., a U.S. Senator from the State of Massachusetts, prepared statement	52
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	3
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont, prepared statement	54

WITNESSES

Davis, Jim, Associate Vice Chancellor, Information Technology, Chief Information Officer, and Professor of Chemical Engineering, University of California, Los Angeles, Los Angeles, California	15
Hoofnagle, Chris Jay, Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic, and Senior Fellow, Berkeley Center for Law and Technology, University of California, Berkeley, Boalt Hall School of Law, Berkeley, California	19
McNabb, Joanne, Chief, California Office of Privacy Protection, Sacramento, California	17
Parnes, Lydia B., Director, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C.	7
Tenpas, Ronald J., Associate Deputy Attorney General, Department of Justice, Washington, D.C.	5

SUBMISSIONS FOR THE RECORD

Davis, Jim, Associate Vice Chancellor, Information Technology, Chief Information Officer, and Professor of Chemical Engineering, University of California, Los Angeles, Los Angeles, California, statement and attachments	28
McNabb, Joanne, Chief, California Office of Privacy Protection, Sacramento, California, statement	55
Mulligan, Deirdre K., Clinical Professor of Law; Director, Samuelson Law, Technology & Public Policy Clinic, Faculty Director, Berkeley Center for Law and Technology, Director, Clinical Program, and Chris Jay Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic, and Senior Fellow, Berkeley Center for Law and Technology, University of California, Berkeley, Boalt Hall School of Law, Berkeley, California, joint statement	62
Parnes, Lydia B., Director, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C., statement	87
Tenpas, Ronald J., Associate Deputy Attorney General, Department of Justice, Washington, D.C., statement	102
Watkins, Bill, Chief Executive Officer, Seagate Technology, Inc., Scott's Valley, California, statement	113

IDENTITY THEFT: INNOVATIVE SOLUTIONS FOR AN EVOLVING PROBLEM

WEDNESDAY, MARCH 21, 2007

U.S. SENATE,
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 2:37 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein, Chairman of the Subcommittee, presiding.

Present: Senators Feinstein and Kyl.

OPENING STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Chairman FEINSTEIN. This Subcommittee will come to order. Senator Kyl and I have participated in this Subcommittee now for something like 12 years, I think.

Senator KYL. Going on 13.

Chairman FEINSTEIN. Going on 13, back and forth. He has been Chair more than I have, but, of course, I hope to change that record. But we have been able to work very well together over these many years, and I appreciate that so much.

Today we are going to talk about identity theft. Identity theft is a crime that has many, many victims, and all of them innocent consumers that can be victims of a theft when a criminal gets hold of sensitive information like a Social Security number, a driver's license, then becomes them and builds up debt in the consumer's name.

The victim might not even know about the problem until he or she applies for a mortgage or a car loan or a job that requires a background check or finds out their credit is really shot. Suddenly, that new house, the new car that is needed for the daily commute, or even the job opportunity is out of reach.

It might be less obvious, but businesses are also major victims of identity theft. Under recent estimates, the business community loses as much as $48 billion a year in fraudulent transactions that involve stolen identities.

And, finally, our economy as a whole suffers from the chilling effect of identity theft. People who are worried about the security of their personal data will avoid making purchases that might put that data at risk.

Commerce on the Internet is stifled. And when consumers have fewer options for online commerce, there is less of the competition that fosters innovation and economic success.

Since the beginning of 2005, which is just a short time ago, over 100 million data records containing individuals' most sensitive personal financial data, health data, other kinds of data, have been exposed due to data breaches. And that works out to about one in every three Americans. It could include the most personal data of many people in this room, and I will bet you do not even know that.

Some people whose data has been breached do not know they are at risk. Some States require notice to affected individuals when a breach happens, and others do not.

I believe it is really important to ensure that people know when their data has been exposed. The law actually allows people to take steps to protect themselves from identity theft, but that is of no use unless somebody knows they are a potential victim or have been a victim. So that is why I introduced the Notification of Risk to Personal Data Act.

This legislation would require Federal agencies and businesses all across the country to give notice of data breaches involving sensitive personal information, unless they concluded—and the Secret Service agrees because they have the know-how—within 10 days that there is no significant risk of harm to the people whose data was breached.

Today we will talk about why this legislation is needed. We will hear from representatives of the Department of Justice and the Federal Trade Commission, which are leading an Identity Theft Task Force that the President created last year.

I am very proud that my home State has been a leader in this fight, and the Nation's first State agency devoted to privacy protection actually opened in California in 2001, and the head of that agency is here as a witness today.

One of the steps that California took was to enact a law that requires businesses and Government agencies to send people a notice when their sensitive personal information is acquired in a data breach.

Because of that notification requirement, in 2005 Senator Kyl and I learned that over 160,000 records with personal data were accessed in a data breach at a company called ChoicePoint. Now, many consumers never even heard of ChoicePoint in 2005, let alone even knew that the company was holding their personal data. Yet on that day over 160,000 people were, in fact, put at risk.

More recently, in November of last year, the University of California at Los Angeles discovered that a computer hacker had accessed the personal records of up to 800,000 faculty, staff, students, and applicants. Now, UCLA fortunately did the right thing. They sent notices to everyone that was affected, so we know it can be done. The University also set up a toll-free hotline for the affected individuals to get more information. An official from UCLA is here as a witness to describe the University's experience and show why it is important to give notice of breaches.

Last year, the Federal Trade Commission received 250,000 complaints of identity theft. And even though California is a longtime

leader in the fight against this crime, five of the ten cities with the highest number of complaints per capita were in California.

The problem of identity theft is persistent, and it is not going to be solved without a strong effort from Congress and from all those who investigate and prosecute identity thieves.

Now, my bill in the last session, Senator Kyl, was included as part of the Specter-Leahy bill on identity theft. It did not go anywhere. I wanted to break just this data breach part free from the bigger bill and get it passed so people could be notified.

This year the bigger bill was introduced with some changes that are problematic, and, therefore, it is stalled. So I have reintroduced this bill separately with the hope that we could at least move this bill so that people whose information was at risk could at least be notified. I think it is pretty much basic and simple, but hopefully we will be able to move it shortly.

I would like to turn it over to you now for any comment you would like to make, and then I will introduce the panels.

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Thank you very much. Senator Feinstein, thank you for calling this hearing and really for years of hard work in helping to lead the effort to deal with identity theft. Much of the legislation that Congress has enacted is due to your initiative and work that we have done here in this Subcommittee. In fact, I had my staff check. We have held eight hearings in the last 9 years in this Subcommittee on the subject of identity theft and financial privacy and security for our citizens, and a lot of the information that has come from the hearings has resulted in legislative activity.

As Senator Feinstein noted, identity theft is one of the fastest-growing crimes, not just in America but in the world. According to an article in the Baltimore Sun, identity theft-related crime cost business and individuals—almost the same number you had—nearly $50 billion in 2006 and an estimated 8.4 million Americans were victims of ID theft in 2006, about 1 in 25 people. If you just stop and think about that, it is a lot, especially if you consider that the young and the elderly are especially targets for this crime.

My home State has the dubious distinction of being, and I will quote from an FTC report from February 7th of this year, "an ID theft hotbed," posting more per capita complaints than any other State in the year 2006. Last year alone, there were 8,146 victims of identity theft in Arizona, the fourth consecutive year Arizona led the Nation in per capita ID theft.

I recently met with Todd Davis, who is the CEO of LifeLock, which is a company that offers a proactive solution for individuals concerned about this problem. For $10 a month, LifeLock will set alerts on a customer's credit reports at each of the major credit reporting agencies, and once the alerts are set, the credit reporting agencies are required to contact a customer personally to verify the legitimacy of any credit activity that is occurring. These alerts, which the company renews periodically, help prevent the unauthorized use of an individual's personal information after that person has become the victim of identity theft.

I mention this just to note that the private sector is coming up with some innovative solutions as well, which, combined with what we are doing here, hopefully can reduce the incidence and the significance of the problem.

According to Arizona Attorney General Terry Goddard, there is a high correlation between ID theft and methamphetamine use. Meth users typically steal identities in order to feed their habits, he says. An October 2006 article in the Washington Post also discussed this relationship and said, "Unlike other drug users, those on meth stay up for days and can become absorbed in methodical, repetitive tasks, creating a high correlation between meth abuse and identity theft crimes."

In fact, an investigation by the Tucson Police Department and the U.S. Postal Service recently led to the arrest of a number of members of an ID theft ring that was mostly made up of heavy methamphetamine users.

Another cause of identity theft in this country is illegal immigration. U.S. Immigration and Customs Enforcement agents recently arrested nearly 1,300 illegal aliens as part of an ongoing investigation into a large identity theft conspiracy. The ICE operation, known as Operation Wagon Train, targeted a large meat-processing company in six States and uncovered illegal workers from eight countries. According to the head of ICE, Homeland Security Assistant Secretary Julie Myers—and I am quoting—"The use of fraudulent documents by illegal aliens seeking employment has been a significant problem. In recent years, however, this fraud has evolved into a disturbing new trend. Now, instead of obtaining fraudulent documents with fraudulent identities, illegal aliens are buying genuine documents using identities of unwitting U.S. citizens."

Terrorism is another cause of ID theft. In 2002, Dennis Lormel, Chief of the FBI's Terrorist Financial Review Group, testified before this Subcommittee that identity theft was a key catalyst for terrorist groups. Also at that hearing, John Pistole, Acting Assistant Director for Counterterrorism at FBI, testified that financing of terrorism is facilitated through identity theft and that terrorists use identity theft to obtain cover employment and access to secure locations.

So we have a multitude of problems and relationships, all nefarious, with this problem of ID theft, and I applaud the Chairman for examining further the adequacy of our ID theft laws today.

I want to tell you also in advance that at 3:15 I am supposed to go to the floor to offer an amendment, so I hope I will be able to at least hear from the first panel, but I might miss the second panel. If I do, I apologize, and I will be anxious to read the transcript of the hearing later.

Thank you again, Senator Feinstein.

Chairman FEINSTEIN. Thank you very much, Senator Kyl.

I thought your comments were very interesting, and I look forward to working with you.

Let me get on with the first panel. I would like to introduce the witnesses. I am going to ask you if you could confine your remarks to 5 minutes so we have an opportunity to go back and forth.

Ron Tenpas is the Associate Deputy Attorney General for the United States Department of Justice. He was appointed in November of 2005. He serves as Executive Director to the President's Identity Theft Task Force. His other duties include coordinating the work of the President's Corporate Fraud Task Force, overseeing initiatives and work relating to health care fraud enforcement, and reviewing legislative and policy proposals to prevent and punish misconduct by corporate and public officials.

Before his appointment as Associate Deputy Attorney General, he served as a U.S. Attorney for the Southern District of Illinois—so we know there is life after—and was an Assistant U.S. Attorney in the District of Maryland and the Middle District of Florida. He was a law clerk to Chief Justice William H. Rehnquist. He is a graduate of Michigan State University, the University of Virginia Law School, and earned a degree from Oxford University as a Rhodes scholar.

Lydia Parnes is the Director of the Bureau of Consumer Protection of the Federal Trade Commission, which is one of the FTC's two law enforcement bureaus. The Bureau is the Nation's only general jurisdiction consumer protection agency. This Bureau enforces a wide range of laws designed to prevent fraud and deception in the commercial marketplace, to protect consumers' privacy, and to provide consumers with important information about the goods and services they purchase.

Ms. Parnes joined the FTC in 1981 as Attorney Advisor to the Chairman. During her career, she has held a number of management positions, including Deputy Director of the Bureau of Consumer Protection from 1992 to 2004. She received her J.D. from the Washington College of Law at American University.

Welcome, both of you. Mr. Tenpas, if you would begin, that would be excellent.

STATEMENT OF RONALD J. TENPAS, ASSOCIATE DEPUTY ATTORNEY GENERAL, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. TENPAS. Thank you. Good afternoon, Madam Chairman and Ranking Member Kyl. I appreciate the opportunity to testify on the important issues that are the focus of today's hearing. Madam Chairman, we are grateful for the Committee's role in addressing the problem of identity theft and appreciate the legislative leadership that you personally have demonstrated in this area. You were a leader in the adoption of the Aggravated Identity Theft Penalty Enhancement Act of 2004, which gave Federal prosecutors important new tools in prosecuting this crime. We have made extensive use of that statute, and the Department of Justice shares your concern and interest in finding new ways to address this problem.

The Department of Justice remains committed to aggressively combating the problem of identity theft working in concert with our many other Federal agency partners, such as the FTC, that play equally important roles. The precise scope of identity theft escapes uniform quantification; however, as you noted, it is clear that identity theft affects millions of Americans every year, cheats Americans of tens of billions of dollars, and as a result, demands contin-

ued attention across Government, in the private sector, and by individual citizens.

The Department has aggressively sought to address this growing problem on parallel tracks. The first is our longstanding and continuing role as the leader of national law enforcement efforts. Our prosecutors continue to investigate and charge criminal identity theft cases every day all across the country, and in my written testimony, I have given a number of examples that range in scope of the cases that our prosecutors have been working on. They do so working closely with our agents in the FBI and with other important law enforcement partners, such as the Secret Service, the United States Postal Inspection Service, the Social Security Administration's Inspector General, and State and local authorities.

Our Department brings cases involving identity theft under a variety of statutes, including mail and wire fraud, statutes criminalizing the misuse of Social Security numbers and of credit cards, and statutes relating to postal theft. And as you alluded to, because identity theft is so often interwoven with other crimes, for example, the methamphetamine problem that you alluded to—that is a matter I am personally familiar with especially in my time as U.S. Attorney in Southern Illinois. Even to concentrate on the fraud statutes probably underestimates the work that we do related to identity theft because so often we are using other statutes to go after people for whom identity theft may be a means to a bigger and even more—at least as important crime.

But let me cite one particular example. We have prosecuted more than 700 of America's most serious offenders in the last 2 years using the new 2-year mandatory minimum penalty that is provided for in the Identity Theft Penalty Enhancement Act, which I alluded to a moment ago and which this Committee and you, Senator Feinstein, led the legislative efforts to create.

Our second role at the Department has been to work closely with our colleagues at the FTC to lead the work of the President's Identity Theft Task Force, which the Attorney General chairs and the FTC Chairman co-chairs. The task force was established in May of 2006 by the President. It is composed of 17 different Federal departments and agencies and is charged with implementing Federal policy to deter, prevent, detect, investigate, proceed against, and prosecute identity theft, focusing on three specific approaches: first is increased law enforcement actions to prosecute identity thieves and deprive them of the benefits of their crimes; second is improved public outreach by the Federal Government to the public and private sector; and third is increased safeguards within the Federal Government to protect the personal data that we in the Government hold.

The task force was specifically charged with producing a strategic report with recommendations for the President for improving the Federal Government's work related to identity theft. The task force is in the final stages of what has been an unprecedented Federal effort to examine the identity theft problem and to identify comprehensive, multilayered solutions to address it. We have convened multi-agency working groups, met with representatives of various groups interested in this problem, invited formal public comment, and we are now in the very final stages and expect the

report to be delivered to the President in mid-April. We look forward to providing the report to this Committee and to public so that we can work with you to address areas of common concern.

Because this area is so important, the task force released a group of seven interim recommendations last September. They focus on the following areas: proposed immediate steps that Federal agencies can take to improve our own practices as repositories of data; urging the Government to sponsor workshops to highlight new identification and authentication technologies that the marketplace is currently producing so that we can promote best practices; and proposing the adoption of new criminal provisions designed to help victims get better restitution and designed to help victims and law enforcement through the creation of universal police reports. All of these interim recommendations either have occurred and been executed at this point or are in the process of being so or doing so.

Again, we thank you, Madam Chairman, for your continued interest and leadership in addressing this complex and pressing issue. We look forward to your questions today, and we look forward to working with you and the Committee going forward. Thank you.

[The prepared statement of Mr. Tenpas appears as a submission for the record.]

Chairman FEINSTEIN. Thank you very much. Good work, and I thank you for your work.

Ms. Parnes, please proceed.

STATEMENT OF LYDIA B. PARNES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, D.C.

Ms. PARNES. Thank you. Chairman Feinstein, Ranking Member Kyl, I also appreciate the opportunity to testify today about identity theft, data security, and the collection, use, and disclosure of Social Security numbers. Although the views expressed in my written testimony represent those of the Commission, my oral presentation and responses to your questions are my own and not necessarily those of the Commission or an individual Commissioner.

Chairman FEINSTEIN. We understand the disclaimer.

[Laughter.]

Ms. PARNES. Thank you. It is—yes, thank you.

Identity theft is a pernicious crime that afflicts millions of Americans and costs consumers and businesses billions of dollars every year. But the damage caused by identity theft, as you indicated, transcends these direct costs. It threatens consumer confidence in the marketplace, especially in electronic commerce, and, Chairman Feinstein, I also thank you for your leadership in trying to address the identity theft problem by introducing bills on breach notification and misuse of Social Security numbers.

There are many causes of identity theft, but I would like to focus today on two of them: the failure to safeguard consumer-sensitive information and the availability and value of Social Security number to identity thieves.

Although not all data breaches result in identity theft, some do. And for that reason it is critical that those who maintain sensitive consumer information adequately protect it. The Commission has

been vigorous both in educating businesses about data security and in enforcing the existing Federal data security laws. We have business education materials on ensuring computer security, complying with the GLB Safeguard Rules, and responding to a data breach. And just this month, we issued a new guide for businesses providing comprehensive advice on developing and implementing reasonable data security procedures.

On the law enforcement front, the Commission has since 2001 brought 14 cases challenging inadequate data security practices. These cases have certain common elements. In each, the company's security vulnerabilities were multiple and serious. The company did not take advantage of readily available and often inexpensive measures to avoid or correct these vulnerabilities. Together, these cases stand for the proposition that companies must maintain reasonable and appropriate procedures to protect sensitive consumer data.

We also must do more to keep Social Security numbers out of the hands of identity thieves, and we must do what we can to reduce the value of Social Security numbers to thieves who are able to procure them. Reducing the unnecessary collection, use, and disclosure of Social Security numbers is a good first step, and the Federal Government has already begun this effort. The Identity Theft Task Force issued interim recommendations in September. One of these recommendations was that the Federal Government review its policies for collecting and using Social Security numbers. The Office of Personnel Management is finalizing its review of the use of Social Security numbers in its collection of human resource data from agencies, with the goal of eliminating unnecessary use.

It is still important to remember, though, that the Social Security number, which is widely used to match individuals to information about them, serves important and beneficial functions in our economy. Excessive restrictions could harm such important purposes as public health, criminal law enforcement, and anti-fraud and anti-terrorism efforts.

Yet even with better security and appropriate restrictions on the unnecessary use of Social Security numbers, some sensitive information inevitably will find its way to identity thieves. For that reason, making it more difficult for criminals to use the information to steal an identity is an essential part of the solution.

Too often, criminals with a stolen, name, address, and Social Security number are able to open accounts in the victim's name. We should do what we can to improve authentication of identities. Next month, the Commission will host a workshop on this subject designed to facilitate the development of improved means of authentication.

Finally, empowering consumers by educating them on identity theft is another important tool at our disposal. The Commission has been a leader in this endeavor. To date, we have distributed more than 22 million publications on identity theft. Our nationwide identity theft education program, entitled "Avoid ID Theft: Detect, Detect, Defend," was launched last year. It includes direct-to-consumer brochures, as well as ready-made kits for organizations to use in training employees or constituencies, complete with presentation slides and a video. Our multimedia website, OnGuard On-

line, educates consumers about basic computer security. And the Commission maintains a hotline and online complaint form through which we receive between 15,000 to 20,000 contacts each week from identity theft victims and those who hope to avoid becoming victims.

Identity theft is one of the most important consumer protection issues of our time. The Commission will continue to place a high priority on preventing this crime and helping victims recover from it. We look forward to continuing our work with you in this effort, and I would be happy to take any questions.

[The prepared statement of Ms. Parnes appears as a submission for the record.]

Chairman FEINSTEIN. Thank you very much for the testimony. I am going to ask Senator Kyl to go first since he has to be on the floor. Senator?

Senator KYL. I really appreciate that. Thank you very much.

First, probably to Mr. Tenpas, but either one of you are welcome to respond, according to the Identity Theft Resource Center, a national nonprofit organization based in San Diego, about 30 percent of identity theft victims have had fraudulent accounts opened in their names after placing a fraud alert. What is the penalty or consequence for a company that extends credit despite knowing of the existence of the fraud alert? And would a consumer have a private right of action against such a business?

Chairman FEINSTEIN. Good question.

Mr. TENPAS. We have been working very closely together. Can we confer for a moment about who is better to take that?

Senator KYL. Sure.

[Laughter.]

Senator KYL. And, incidentally, I am not trying to play "Stump the Witness" here. If you get any ideas that you would like to present to us later, that would be fine, too.

Mr. TENPAS. We have been pretty closely joined at the shoulder over the last 10 months, so if you will give us a moment.

Ms. PARNES. Yes, I can—

Mr. TENPAS. I will defer to my learned colleague.

Senator KYL. OK, good.

Ms. PARNES. The 30-percent figure is a familiar one. Most of the surveys that have been conducted indicate that about 30 percent of the victims have been the subject of what is called "new account fraud." But what I actually have not heard is that these have been accounts that have been opened after alerts have been placed. That is actually new information, and I would like to go back and look at that, if I may.

Senator KYL. Sure. I will provide you the—this comes from the Identity Theft Resources Center, a January 2007 article. I can give you the citation for it. So maybe what you could do is take a look at that and then get back with any information that you can.

Ms. PARNES. OK. Thank you.

Senator KYL. Thanks. And this is kind of a followup. Various companies—and I mentioned one—offer services that—well, actually, this is a different point, but offer services that provide addresses, criminal, civil, and professional history as well as a list of assets and bank account numbers. You are familiar with these.

Also available are Social Security numbers, current phone numbers, names and phone numbers of neighbors and family member names.

What protection is needed so that credit bureaus and information agencies are prohibited from selling such personal information?

Ms. PARNES. Well, I certainly think that the restrictions on Social Security numbers that are included in this bill are a start in limiting the sale and disclosure of Social Security numbers.

Senator KYL. Have the credit bureaus been working closely with FTC to address these kinds of problems?

Ms. PARNES. We work very closely with the credit bureaus. Yes, we do.

Senator KYL. I think that is important. The President's ID Theft Task Force is something else that has at least been in existence. Do you know what type of input the task force has sought from different consumer groups and private sector groups? It seems pretty heavily Federal Government oriented.

Ms. PARNES. Well, the task force—we have spent a good deal of time talking among the 18 agencies that are members of the task force. But we also had a period of time when there was public input that was sought. Notice was given, and we received—

Mr. TENPAS. We had about a 2-month public comment period. We set that public comment period once the task force had begun its work, and rather than simply inviting general comment—you know, "Tell us what you think about identity theft"—we tried to identify eight or nine broad areas where we thought a lot of the task force work was being focused.

A set of the questions essentially invited comments in the area you have described about what, if anything, remains to be done in terms of establishing regimes for businesses about protecting data, providing notification, and uses of that data. And I think within the task force there has also been a recognition that, as Lydia referred to, there are important legitimate uses of Social Security numbers, and one of the things that is important to do is make sure we have a good grasp of the legitimate—all of the ways in which Social Security numbers and other sensitive data are being used and shared, so that you can then parse out which ones really benefit consumers, which ones potentially make businesses better able to meet consumer needs, and which of those are sort of historic curiosities that grew up because, for example, a Social Security number was the easiest identifier at the time but where we have now got better ways to go about that.

Senator KYL. A very good way of distinguishing these different uses. Just to mention a final point, we are in very detailed discussions with members of the Department of Homeland Security and the Department of Commerce, and they have in turn got conversations going with the Social Security Administration and others about the Social Security number data base as it relates to enforcement of the immigration laws and potentially a new employee verification system that could be put in place as part of a comprehensive immigration reform. Clearly, we are going to have to have another whole conversation about that, and you all will be important in that.

Senator Feinstein, I am sorry. I will have to go.

Chairman FEINSTEIN. I am sorry, too.

Senator KYL. But thank you for allowing me to go forward here, and I appreciate it very, very much.

Chairman FEINSTEIN. If you can come back, please do. Thank you.

For either one of you, let me ask this question: Any data breach notification statute has to strike the right balance, and this is more difficult than people might think. If notices are sent even when a breach poses no risk of harm, consumers tune it out. Yet if notices are only sent when there is a high likelihood of harm, notices will not be sent often enough because in many cases it will be hard to predict whether the data will be used for identity theft.

The data breach bill that we have introduced requires that notice of a data breach be given unless the breached entity conducts a risk assessment and concludes that there is no significant risk of harm to the affected individuals. So the burden is put on the entity that makes the money by selling this information.

The entity that suffered the breach is also required to send that assessment to the Secret Service, which can overrule the assessment and require notice to be sent to the affected individuals.

Do you believe that it is appropriate to require notice unless there is no significant risk of harm?

Mr. TENPAS. I think the general approach that you have described is one that actually is already reflected in some of the task force's own work. One of the things that occurred as part of the interim recommendations that I alluded to was that the task force prepared guidance for Federal agencies to serve as, you know, something of a playbook for a Federal agency if it had an incident where sensitive information may have been compromised. And one of the things that that guidance recommends is to conduct an analysis of the kind you have described, not to sort of jump to the conclusion that every time information may have been—"compromised" may not be quite the right word—but some way there is some level of loss of control of it, you do not immediately jump to notification because, as you say, I think there is a very substantial concern that consumers will grow immune to notices and not be able to distinguish really important ones from less important ones.

So I would say I think generally the approach you have outlined is one that the task force has already thought about and is one that we have sort of embraced for the Federal Government itself.

Chairman FEINSTEIN. I really appreciate that because this has been difficult, as you probably know, to work out. But in retrospect, as I look back on it, it seems to make the best sense as a way to do it.

Mr. TENPAS. Senator, could I make one other just very small point on that?

Chairman FEINSTEIN. Sure.

Mr. TENPAS. I think there are a couple of other things that are reflected in that that are useful. One is the notion of a notification to law enforcement so that they are able to involve themselves in a timely way in trying to figure out what the potential criminal opportunities might be from a particular incident. I think from a Department of Justice angle, we would also just note that the FBI is

a very important investigative agency in parallel with the Secret Service, and so we think it would be useful for there to be some recognition of that in terms of any kind of notification or law enforcement kind of vetting.

Chairman FEINSTEIN. I would be open to any suggestion you might make. We chose the Secret Service because they apparently have the know-how to do this and can do it. But if you have a recommendation, I would sure welcome it.

Mr. TENPAS. OK. Thank you.

Chairman FEINSTEIN. We want to make this as good as we possibly can.

Mr. TENPAS. And the Secret Service does have tremendous expertise. That is not meant, you know, in any way to suggest they do not. But this is an area where a number of agencies all play important roles. Some have closer ties to one industry sector than another, and so I think we just want to be sure that anything we do here, we capitalize on the collective talents and abilities of all those agencies.

Chairman FEINSTEIN. I think one of the things that I have been interested in is, for example, I did not know that every time I buy something out of a catalogue or use my credit card or virtually do anything, it all goes into a big data grist mill, and the information is all compiled, and companies sell this information to other people. And almost nothing is private anymore.

All your financial information is easily available and can be used. If somebody gets your driver's license and your Social Security number, they can go to this financial information and rip off people to the tune of hundreds of thousands of dollars.

Do you have any other suggestions, either one of you, as to what we might do in this? Now, I know that L.A. County has set up an identity theft unit to service people who have had these problems. But it is very hard. I have talked to people where it has taken 18 months to recover your identity, and during that period of time, you were almost a non-entity. You have no credit. You cannot do this or that.

See, I think that if you are going to sell somebody's personal data, you ought to have their permission. And that is the old opt-in/opt-out argument, and business resists it.

That is the only answer I know.

Ms. PARNES. I think, you know, a couple of things. The risk of lost or stolen information in our experience at the Commission, you know, goes beyond the situation that you were describing where your data is compiled, your personal financial information is compiled somewhere, and that it can be sold among entities. But what we have seen is the risk that exists when retailers are holding information. I mean, many of the cases that the Commission has brought involved data breaches at retailers—retailers that held information, credit card account information.

Chairman FEINSTEIN. Give an example of that, would you?

Ms. PARNES. Well, you know, one example is the case—well, certainly one example was the ChoicePoint case that you mentioned. But another one was a case we brought involving BJ's Warehouse, a store, and they held information—they held credit card information when consumers paid for that information, and they were—

that information was hacked by someone who was able to get into the system through the store scanners. It was a vulnerability in their system. So someone was able to get into their system and get all of this credit card account information.

Now, a couple of problems there. First of all, retailers have no need to hold that account information for a particularly long period of time, and some do, and that is a problem.

Chairman FEINSTEIN. I think a lot do.

Ms. PARNES. Yes.

Chairman FEINSTEIN. The question is: What do we do about that?

Ms. PARNES. Well, you know, one of the things that we have been trying to do in our cases is highlight what the problems are and get out then consumer—excuse me, business education material really alerting the business sector what are the do's and don'ts in terms of data security. And the recent brochure that we released earlier this month I really think is an excellent example. We talk about tossing information. Don't keep it if you don't need it. Really look at what you need.

Chairman FEINSTEIN. Well, let me give you an example. I went into a store here not long ago, and the individual that waited on me—they knew I was coming in—knew everything I had bought on the other side of the country. I was sort of staggered by that.

So I say to everybody out there, there are no secrets anymore. Everything is an open book, and I really have some concerns. I do not know what I think of that in terms of privacy being so violated all the time.

Mr. TENPAS. Senator, could I add just one or two observations on that as well? I think we share that concern. One of the aspects of this problem that is, I think, so difficult to wrestle with is that same phenomenon that you describe of sort of the information being everywhere, also in certain cases presents opportunities to help consumers.

As an example, one of the things we have been looking at in connection with the task force is thinking about, you know, in those unfortunate cases where a Government agency has an incident and some information is lost, how you respond to that. And one of the things that has happened during the life of that is a number of business enterprises have stepped forward to point out that they believe they have technologies or systems that, sort of capitalizing on the fact that a lot of information is out there, allows them to track whether a particular data breach is leading to identity theft.

Chairman FEINSTEIN. Right.

Mr. TENPAS. So, you know, this is a sort of short layman's summary of it, but if 10,000 names or records were kind of lost, there are businesses now that believe they can, if you give that information to them, essentially go out and monitor what is going on in the world in terms of new accounts being opened, purchase activity, and detect unusual surges that would suggest that the information that has been compromised is actually being used for identity theft, because, obviously, the compromise is not the same as a person taking it up and misusing it.

And so one of the really hard problems here is the things that create risk for us also create some opportunities to help consumers. And so getting the balance right is a difficult one.

Chairman FEINSTEIN. Let me ask you for your advice. Do you think we should pass legislation that would require Federal agencies to give notice of a data breach?

Mr. TENPAS. I think our sense on that is that you should give us some chance, through the task force and other places, to get policies in place. I think one of the concerns about sort of legislating in this area is it is changing so quickly.

Chairman FEINSTEIN. Yes.

Mr. TENPAS. For example, the ability that I described to you was not one that certainly I was aware of and I do not think was well developed even perhaps 2 years ago. And so I think what we want to really be encouraging in the Federal Government is for our agencies to be adopting the best possible practices available at any moment. And what those are today, you know, I am not a big gambler, but I would be willing to bet that whatever those are today, 2 years or 3 years from now we are going to think there is something even better and smarter that you can do. And sort of allowing us—

Chairman FEINSTEIN. That is a pretty good non-answer.

Mr. TENPAS. Well, I think it is—

Chairman FEINSTEIN. I take it the answer is no, you do not think we should.

Mr. TENPAS. I think we would like some time—

Chairman FEINSTEIN. OK. Fair enough.

Mr. TENPAS.—to sort of try to manage our affairs and see if we can come up with ways to be responsive.

Chairman FEINSTEIN. Fair enough. That is why we tried to keep this bill simple, just data breach notification, and at least get that first step of protection out for the consumer. I just hope we can pass the bill. Anything both of you can do to be supportive would really be appreciated. I would like to get it passed as soon as possible, as a stand-alone bill if we have to, at least so there are some specifics out there with respect to notification in the event of a data breach, instead of having different States doing a different thing.

Mr. TENPAS. Right.

Chairman FEINSTEIN. So let me just thank you for your testimony. Unless you have another comment you would like to make, we will move on to the next panel. You have been very generous, and we appreciate it.

Ms. PARNES. Thank you.

Mr. TENPAS. Thank you very much, Senator.

Chairman FEINSTEIN. Thank you.

All right. This should be a very interesting panel, and I will introduce the individuals. In particular, Mr. Davis, let me thank you for coming such a long distance to be here today. I will begin by introducing you.

James Davis is the Associate Vice Chancellor, Information Technology, and Chief Information Officer of UCLA. Mr. Davis will describe the data breach that UCLA discovered in November of 2006. He is a professor in the Department of Chemical and Biomolecular Engineering at UCLA. In his Associate Vice Chancellor position, he has broad responsibility for University-wide technology planning

and implementation oversight. That means he is the point man there. He both facilitates and coordinates the campus IT planning, policy setting, prioritization, and decisionmaking processes, and is responsible for the strategic deployment of academic and administrative operations, services, and resources in support of the University, which is a big University, and its central and distributed technology requirements. He is responsible for UCLA's Office of Information Technology and coordinating IT deployment.

Joanne McNabb is the Chief of the California Office of Privacy Protection that was created by legislation and opened in 2001. It is the first in the Nation, and it is a resource and advocate in identity theft and privacy issues. Mrs. McNabb is a certified information privacy professional, is co-chair of the International Association of Privacy Professionals' Government Working Group. She also serves on the Privacy Advisory Committee of the United States Department of Homeland Security. Before starting the Office of Privacy Protection, she had 20 years' experience in public affairs and marketing, in both the public and private sectors. She attended Occidental and holds a master's degree, of all things, in medieval literature from the University of California at Davis.

Chris Jay Hoofnagle is the Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic. He is a senior fellow at the Berkeley Center for Law and Technology, the School of Law, Boalt Hall, University of California. He previously served as director of the West Coast office and senior counsel at the Electronic Privacy Information Center. He is the author of many scholarly articles on identity theft and privacy protection and has served as a witness and commentator on privacy issues in Congressional Committees, State legislative bodies, and major media.

Thank you, all of you, for being here. You have all come a distance, and we really appreciate that on this first day of spring. So let's begin with you, Mr. Davis.

STATEMENT OF JIM DAVIS, ASSOCIATE VICE CHANCELLOR, INFORMATION TECHNOLOGY, CHIEF INFORMATION OFFICER, AND PROFESSOR OF CHEMICAL ENGINEERING, UNIVERSITY OF CALIFORNIA, LOS ANGELES, LOS ANGELES, CALIFORNIA

Mr. DAVIS. Thank you, Madam Chair. Obviously, I am here because UCLA, as noted, was the recent victim of a large data base security breach and reached the decision to notify more than 800,000 people that their Social Security numbers were or might have been illegally accessed. The scale and complexity of the situation served to amplify a number of difficult questions during deliberations, the intersections of competing goals, and the important elements of notification. So my objective today is to share some of our key experiences in light of the California law that I believe bear on the proposed legislation.

I would like to start by saying we were thankful that we had a well-established incident response policy, process, and protocol in advance of the breach. Given the complex technical environment, the forensics picture evolved over multiple weeks, rapidly changing our understanding of the nature and sophistication of the attack,

and dramatically affecting the number of potentially affected individuals.

By UCLA policy, the final decision to notify rests with me as the Chief Information Officer. I convened what I considered to be the most objective, independent panel to help reach a final decision. The panel included the director of IT security, the director of IT policy, the campus network architect, legal counsel, and the University of California director of IT policy, as well as the director responsible for the particular data base.

We needed to meet repeatedly, and our deliberations involves systematically reviewing the technical evidence, the projected approach of the hacker, and the intent of the attack. These were reviewed against the notification criteria from integrated technical, policy, and legal viewpoints. And I want to stress that the ability to analyze the situation from these viewpoints simultaneously was critical.

A key lesson involved also was the tension in maintaining confidentiality while the investigation was in progress. We were keenly aware that the information going out prematurely or inappropriately could expose our systems to further harm or adversely impact notification. At the same time, we wanted to share information, especially technical information, quickly with others who could benefit. Ultimately, we were able to conclude with confidence that a very small percentage of the 800,000 individuals in our data base required notification under California law. There was not conclusive evidence, however, of access for the rest. Therefore, the more difficult decision became whether to notify the rest of the individuals, the vast majority, when we knew doing so would have a large impact on them and on the campus.

We used additional criteria—duration of exposure and the targeted nature of the attack—to help think through the situations where technical proofs were inconclusive. These are criteria articulated as guidelines by the University of California and drawn from Joanne's office.

There was also a larger philosophical question about UCLA's position. Individual privacy is an institutional value highly regarded by the University of California and deeply embedded in our policies. There was early on a consensus that ensuring people are in the best possible position to protect their information indeed supported this value. Providing broader notification than was strictly required legally was part of this position.

At the point of notification, it was critical to have the call center and website fully ready to go. We had 12,000 calls the first day. At its peak the call center operation included 1,600 non-dedicated operators at 26 locations, handling as many as 1,000 calls per hour. Our website averaged 15,000 daily visitors during the first week of notification. We want to stress the importance of solid information, especially the ability to confirm a name in the data base and the specifics on how to protect oneself from identity theft. We were continually updating information in response to questions and reactions.

We identified three groups of callers. The largest group felt violated and anxious and wanted the connection with a live person for answers and empathy. A much smaller group just wanted informa-

tion. And about 2 percent of the callers were sufficiently angered or distraught that they demanded to speak with a higher-level UCLA official. Defining the escalation process was key to handling this last group of callers and essential to a successful notification process.

Our experience left no doubt that notification effectiveness was determined by the ability to reach someone knowledgeable and/or to quickly find useful information for taking action; designed to minimize busy signals, voice messages, providing up-to-date information, and ensuring sympathetic operators were also very important. In terms of actual notification, all channels were important: e-mail and the media for the fastest way to reach individuals, and U.S. Mail for the more personalized notice.

The enactment of the 2003 California law has empowered individuals to protect themselves against identity theft, and we want to also note it caused the University of California to accelerate and intensify institutional efforts to protect data. The fundamental belief is that the best protection, however, is not to have the protected data at all. Since 2003, UCLA has put significant effort into reducing the retention of Social Security numbers for all internal business practices. The same is true for the other UC campuses.

In light of the breach, we have examined why we keep Social Security number institutionally, and we find it is because we must provide them to external organizations, such as the Internal Revenue Service and the National Student Clearinghouse. Though we continue to eliminate the unnecessary internal use of Social Security numbers, we see a threshold beyond which we will no longer be able to do so without reduction in the requirements from the external organizations. As the FTC's recent recommended practices and guidelines indicate, an incident response protocol is obligatory, no matter how well one protects data. However, incident response is the last step. We believe that an effective partner to the incident response and notification would be a reduction in these external requirements.

Thank you very much for the opportunity to share these experiences.

[The prepared statement of Mr. Davis appears as a submission for the record.]

Chairman FEINSTEIN. All 800,000 were notified?

Mr. DAVIS. All 800,000 were notified.

Chairman FEINSTEIN. Thank you. Joanne, welcome.

STATEMENT OF JOANNE MCNABB, CHIEF, CALIFORNIA OFFICE OF PRIVACY PROTECTION, SACRAMENTO, CALIFORNIA

Ms. MCNABB. Thank you very much. Thank you, Chairman Feinstein. I am very happy to be here. As you mentioned, the California Office of Privacy Protection is an education and advocacy office; that is, we do not enforce any of California's privacy laws. Our mission is, rather, to identify consumer privacy problems and to encourage fair information practices.

We have four main functions: We assist consumers, and others, who call our hotline or e-mail us. We provide a lot of educational and informational tools, documents, a lot of workshops. For example, this year we are doing a series of victim assistance training

programs for community-based organizations to help us reach groups that we do not routinely come across. We work with law enforcement, particularly on identity theft, and also on security incidents. We are just about to release a training manual for law enforcement on investigating and prosecuting identity theft. And, finally, we make best-practice recommendations to organizations on how to handle personal information in ways that reduce the exposure to identity theft for the people whose personal information is involved. One of our sets of recommended practices is related to breach notification, and we issued that one in 2003.

Identity theft has been a major focus of the office from the beginning. In fact, about 60 percent of the calls that we get are about identity theft. Fortunately, only about 8 percent are from victims. The rest are from people who perhaps got a breach notice or saw a television ad or a news story that made them concerned about identity theft.

California, as you mentioned, has indeed been a leader in privacy protection, and many of the more than 80 significant privacy laws introduced—enacted, actually, since 1999 have been imitated by other States and are receiving some consideration here in Washington. I want to just highlight three briefly, all of which were inspired by concerns about identity theft.

The first one is a law relating to Social Security number confidentiality, which took effect started in 2003, which prohibits the public posting or display of Social Security numbers. It is because of that law that I no longer have my Social Security number on my Blue Shield card, nor do the other members of my family who used to have my Social Security number on their Blue Shield cards. Similarly, it is no longer on student ID cards, and every professor no longer has to receive the Social Security number of every student in his or her class. So that cut at dealing with Social Security numbers is aimed at removing them from public view, to some extent.

The second law that I think has had a significant impact on identity theft is the security freeze law which allows individuals to have control over who gets access to their credit files, which are full of sensitive personal information, including Social Security numbers. This law has been in effect since 2002 and gives consumers the most effective tool available to them to protect themselves against new account identity theft, which, as Ms. Parnes mentioned, is one of the most difficult kinds to recover from.

And then, finally, we come to the best known California privacy law, the breach notice law, which was indeed inspired by a concern about identity theft. A look at the legislative history reveals that the way it was described as a means of giving consumers sort of early warning so that they could take defensive action because their information was exposed in a way that put them at risk of identity theft. That was the way they talked about it as they were passing it.

I think, however, the real impact of the law has been the extent to which it has served as a stimulus to organizations to improve their practices for handling personal information and that that has been the biggest impact. One way to look at it is that the notification process, the requirement to notify, revealed the cost of insecu-

rity. Before that it just seemed like information security was just a cost that did not have any benefit. Well, now there is a cost to not securing information, so we can look at spending some money to protect it.

I want to mention a couple of examples that we have learned of about the way in which organizations have changed their practices because of the breach notification requirement, and UCLA is an excellent example. It was not only a very good response on so many levels, being genuinely helpful, using multiple communications channels, offering people information about the security freeze, which is much more effective to protect them than credit monitoring and using the call centers so effectively, but principally, I want to commend their dedication to looking for ways to reduce the presence of Social Security numbers even further than they already have.

We have seen similar actions in a couple of other organizations, which I do not think I will go into right now.

So I would like to, in closing, quote another UCLA professor, Phil Agre, who says that personal information is like toxic waste, it takes skill and training to manage it, and to suggest that sometimes the best way to manage it is to detoxify the waste stream.

Thank you.

[The prepared statement of Ms. McNabb appears as a submission for the record.]

Chairman FEINSTEIN. Thank you very much, Ms. McNabb.

Mr. Hoofnagle?

STATEMENT OF CHRIS JAY HOOFNAGLE, SENIOR STAFF ATTORNEY, SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC, AND SENIOR FELLOW, BERKELEY CENTER FOR LAW AND TECHNOLOGY, UNIVERSITY OF CALIFORNIA, BERKELEY, BOALT HALL SCHOOL OF LAW, BERKELEY, CALIFORNIA

Mr. HOOFNAGLE. Thank you, Madam Chair. Let me say that it is very nice to see you so well ensconced in that chair and in possession of the gavel.

Chairman FEINSTEIN. Thank you.

Mr. HOOFNAGLE. Thank you for inviting me to this hearing. Let me mention two procedural issues. My written testimony is joined by Professor Deirdre Mulligan. It is not well known that Professor Mulligan at the University of California was one of the architects of security breach notification law in California. She provided a theoretical basis for it and helped then-Assemblyman Joseph Simitian introduce AB 700, which eventually was passed as Senate bill 1386. So we have a deep history in working on security breach notification at the law school at Berkeley.

The second issue I wanted to mention is that our work is supported by the National Science Foundation, and we continue to be dependent on public funding for research, and it is a very important issue to us.

With that, I just have a short amount of time today, so let me mention four of the recommendations we make in our written testimony. We actually make six all together.

Our first recommendation is that Congress should consider the broad beneficial effects of security breach notification. These laws

do not just shield individuals from identity theft. They perform a lot of other functions. And perhaps the best way to illustrate this is to visit environmental laws for a moment.

Professor Mulligan borrowed the idea for security breach notification from environmental right-to-know laws, laws that required registration of dangerous chemicals and then public reporting once those dangerous chemicals were released. Security breach notification laws perform many of the same functions as these environmental right-to-know laws. They address a form of information pollution, if you will, just as Joanne alluded to in Phil Agre's comment. So not only do they warn individuals of risk, they do other things. Breach notification has caused a serious increase in investment in security. Prior to the passage of these laws, companies could simply not disclose security breaches and let consumers bear the costs of identity theft and other harms. But now those costs are internalized, and businesses have to do more to protect data.

Second, one of the best aspects of security breach notification laws is that they are so-called lightweight regulatory mechanisms, meaning that the Government does not dictate how an entity should protect information. They simply say, "agency or business, you figure out how to protect security and privacy, but if it does not work, you have to tell the public." And that is a major benefit of these laws.

Third, just as environmental right-to-know laws reduced inventories of toxic chemicals, one of the things we are seeing is that security breach notification is reducing reliance on sensitive personal information. Now, as Jim noted in his testimony, entities cannot always get rid of all sensitive information. Sometimes it is external entities that are requiring them to hold Social Security numbers and other information. However, these laws are encouraging businesses to go through the process of determining whether or not they actually need Social Security numbers and removing them from their data bases if they can.

Finally, security breach notification laws are very valuable in that they provide benchmarks for performance. One of the problems in investing in security is there are not good metrics to show that security is worthwhile, and having a security breach is a metric. It is a benchmark that can be looked at and can cause re-evaluation and greater security.

Our second recommendation is that the Committee require standardized, central, and public reporting of breaches, just like environmental right-to-know laws. In the appendix to our written testimony today, we have a standardized form from the State of New York which the State requires when you have a security breach. That form sets forth basic information about the breach, how many people are affected, when notice is going to be given, et cetera. And those forms are essential for the public to learn more about breaches, for security researchers to learn about other incidences and whatnot. We really think it is essential that some type of public reporting be included in your bill.

And then, finally, as I am running out of time here, let me just mention that just as security breach notification has given us more information about security lapses, if we had reporting on identity theft incidences, that is, if lending institutions were required to

publicly report about how often they experience identity theft and the vectors of the crime—that is, the types of products that are taken advantage of by criminals—I think we would get a clearer picture of the identity theft problem. And consumers could actually decide which bank to us based on the bank's rates of identity theft, and we could actually have competition.

And with that, allow me to thank you again, Madam Chair, for holding this hearing.

[The prepared statement of Mr. Hoofnagle appears as a submission for the record.]

Chairman FEINSTEIN. Thank you.

Now, let me ask each of you a few questions, if I might. Let me begin with Mr. Davis.

Mr. Davis, would a standard that requires notification of a breach, unless there is no significant risk of harm, be a useful and meaningful standard for entities that are deciding how to respond to a breach?

Mr. DAVIS. I need to give you a mixed answer. In our particular case, the forensics were very complicated, and as I mentioned in the testimony, we had the vast majority of the people, you know, who were faced with the decision about whether to do this. So the really hard question was this risk analysis that you are speaking to.

And so there is the question of how can one put the criteria together and in such a way that this risk analysis can be done in a uniform and a good way. So I raise that question. The principle of it makes good sense to us. How to do it in practice is the question I am raising.

Chairman FEINSTEIN. Well, this would depend upon the nature of the breach and the data, it would seem to me. Perhaps I am all wet, but can you come up with a better standard? This is where we get into, you know, dicey water because this is not something that has not been well considered and kind of vetted with various groups. And it is really the best we have been able to come up with.

Perhaps, Ms. McNabb, would you like to get involved in this part of it?

Ms. MCNABB. I can speak to the issue, not any specific legislative proposal. I think that, in fact, Jim's discussion of the deliberative process they went through is very illustrative. In California, State agencies are subject to notification, so I have been involved in some deliberations similar to that in California, and—

Chairman FEINSTEIN. But we are talking about writing laws for everybody.

Ms. MCNABB. Exactly. I know, so I just want to say that how you conduct the risk analysis can be very tricky. Finally, you may find yourself—

Chairman FEINSTEIN. But that is up to the company or the university or—

Ms. MCNABB. You may find yourself in a position of trying to prove—establish a negative. His case was one example. Some other ones I can think of are where what the forensic evidence shows is that the apparent purpose of a hacking, let's say, was to store pirated music and there was no indication that data that was also

on that server was touched, but there was no indication that it wasn't touched. So then you don't have forensic facts that tell you, yes, that data was accessed or acquired or, no, it was not. So then you have to go to a next level that is not part of risk—well, maybe it is part of risk analysis, but it is part of what are our values and principles and do we believe in an abundance of caution or not.

Chairman FEINSTEIN. What we do, by the way this is worded, is leave it up to the entity to make those decisions rather than to legislate a protocol which might work for some and not work for others. I do not know how we could legislate a protocol.

Ms. MCNABB. Yes. I do not either.

Mr. DAVIS. That is, in effect, what I am saying. It seems very difficult to legislate a protocol.

Just to build on what Joanne said, in our particular case we did have to apply additional criteria, as I said. These had to do with an analysis of the targeted nature of the event, the duration of the event, and our campus position on this. Those were the three ingredients that actually led us to proceed with the notification.

I can certainly think of different situations, for example, with a stolen laptop, then the situation becomes very different, and you can have a very different kind of risk analysis. But if you are saying, you know, the principle of this, that does make very good sense to this, and it does put the burden back on us to do that kind of analysis, which I think that is where it needs to rest.

Chairman FEINSTEIN. I do not know a better way of doing this than saying no significant risk and that the company has to certify that. And that goes within 10 days to the Secret Service with the facts, and they then can reverse that. Let's say the company says there is no significant risk. Then there is a check that says, yes, you have to notify, and that check would be the Secret Service evaluation.

Mr. DAVIS. If I may make one other comment, I may have been answering the question just a little bit differently as I listen to what you are saying. We would actually agree with what you are saying, and that is a good principle to proceed by. What I was really trying to say is that the definition of "significant risk" is very, very difficult, and so when we do our own analysis, it actually is going to be very difficult to find a situation in which we would not notify.

Mr. HOOFNAGLE. Madam Chair, if I may make two recommendations—

Chairman FEINSTEIN. Well, my staff just put a question before me which is interesting. Do you suggest then that the law include criteria for assessing the risk? Even that, I do not know how it could be complete because there are such differences.

Mr. DAVIS. There are people to my left that can speak to this. My own perspective is that it would be very difficult to put criteria together, but I think some criteria based on the experiences across multiple breaches, much like Chris and Joanne have talked about, can be put together that would be useful for us to do our risk analysis and help us do this as an internal exercise.

Chairman FEINSTEIN. Would you be willing to make some suggestions?

Mr. DAVIS. Well, I am trying to suggest two that did work very well for us, which was the targeted nature of the attack as well as the duration of the attack in the particular kind of event that we experienced. Those would be examples of these kinds—

Chairman FEINSTEIN. So you are saying, in other words, that there must be a protocol set up that covers such things?

Mr. DAVIS. That is right.

Chairman FEINSTEIN. OK. Anybody else like to comment on that point?

Ms. MCNABB. I think Jim's testimony actually lists the number of criteria that they had before and that they developed afterwards that would be worth looking at.

Chairman FEINSTEIN. How about misplaced rather than stolen?

Ms. MCNABB. The California law, the triggering event is that data is acquired by an unauthorized person.

Chairman FEINSTEIN. That is a good definition.

Ms. MCNABB. Not "accessed" but "acquired." As it moved through the legislature, it started as "accessed," and that was considered not as good an indication of risk as acquisition. So that can help in some situations.

Chairman FEINSTEIN. For example, what do you do, somebody is traveling—

Ms. MCNABB. Yes, and they lose their laptop.

Chairman FEINSTEIN. They are carrying a computer that has a huge data base in it, and they misplace it.

Ms. MCNABB. Well, you have to decide if you have reasonable belief that it has fallen into the hands of an unauthorized person.

Chairman FEINSTEIN. You would have no way of knowing.

Ms. MCNABB. Right. So you have to—

Chairman FEINSTEIN. So you would have to proceed, it would seem to me, to provide some notification.

Ms. MCNABB. That tends to be what happens.

Chairman FEINSTEIN. Because you cannot take the risk.

Ms. MCNABB. Something like, I think, 46 percent of the notification—of about 530 notifications that we have noted, 46 percent of the time it was a lost or stolen computer or CD or server.

Chairman FEINSTEIN. That is exactly right, and it seems to me that companies have to recognize that their employees, if they carry around these data bases, that is one policy question. Then they have to be responsible—

Ms. MCNABB. And then they can encrypt them.

Chairman FEINSTEIN.—if a computer is misplaced or lost or stolen.

Ms. MCNABB. And the data an be encrypted. California government established a policy that sensitive personal information on portable computing or storage devices must be encrypted.

Chairman FEINSTEIN. That is a good thing to have in our law.

OK. Mr. Davis, was the toll-free number a successful way for affected people to communicate with the University? And how many actually used it?

Mr. DAVIS. Well, let's see. We had a total of about 36,000 calls to the call center over the entire time, so we had quite a few people out of the total number using that call center.

In terms of useful, I would use stronger words. I think it was essential to have the call center and to have that toll-free number. When we look at the responses from the people—and we did track this very closely -people really did want to talk to people, as I said, and the call center was essential to getting information out.

Of course, there were many people that did not have access to a computer or did not have other means to get information, and it proved to be the only way to get information through some of the people who were involved.

Chairman FEINSTEIN. Right. Do you believe that providing an e-mail address to which individuals could write for more information about a breach would be as effective as a call center? And, everybody, please chime in.

Mr. DAVIS. I do not. I think it is a useful second layer mechanism, but I believe the call center—our experience would say—I should not even say "I believe." Our experience would say that the call center was essential as a first line of communication in this kind of situation.

Ms. MCNABB. That is our experience, too. My office has gotten lots and lots of calls over the years from people who got notices, and your statistics were very similar to what ours have been. A lot of people get a letter, and it says something that sounds a little frightening, and they want to talk to somebody.

Chairman FEINSTEIN. Yes, I understand.

Ms. MCNABB. And what the people are saying on the phone is pretty much what it said in the letter, but they want to get it from a live human being.

Chairman FEINSTEIN. Right.

Do you have a comment?

Mr. HOOFNAGLE. It does make sense to have multiple channels available to victims, whether it is e-mail or telephone or the Internet.

Chairman FEINSTEIN. OK. Should notice be required when a breach involves a hard-copy printout of computerized data?

Ms. MCNABB. that is the policy for California State agencies. The policy is that when the kind of information that would require a notice in electronic form has been acquired by an unauthorized person, if it is in paper form we would notify the same way.

Chairman FEINSTEIN. Mr. Davis?

Mr. DAVIS. We are treating it exactly the same way.

Chairman FEINSTEIN. OK. Well, we have covered the lost or stolen laptop. Perhaps you could give us some help on this, and that would be the wording to ensure that it covers not just hacking incidents, but also breaches that involved hard-copy data and lost laptops?

Ms. MCNABB. Well, the California law, when it says "acquisition by an unauthorized person," has been constantly interpreted to apply to lost or stolen laptops or other devices.

Chairman FEINSTEIN. So the whole thing.

Ms. MCNABB. Yes, because—

Chairman FEINSTEIN. The California law, the wording has—

Ms. MCNABB.—it says if the data—

Chairman FEINSTEIN.—been legally interpreted to—

Ms. MCNABB. It has been interpreted by behavior, that is, people since the beginning, those who have had breaches, whether it was a stolen laptop or lost hard drive, have considered that acquisition, apparently, because they notified. There have been proposals in the California Legislature several times since the law was first enacted to remove the word "computerized," because it says "computerized data." So it would just say "data," which would make it clearly apply to paper, and those have never been passed. They were objected to.

Chairman FEINSTEIN. Right. That is interesting. All right. If any of you have a comment you would like to make, we will conclude this, but I would like to ask that if you have not had a chance to look at the bill, that you perhaps do so and give us any comment you might care to make, how to strengthen it or better it in any way. Any comments?

Mr. HOOFNAGLE. Madam Chair, may I make one comment? That is, there is an exemption for situations where there is no significant risk of harm that would exempt a company or an agency from giving notice.

Chairman FEINSTEIN. Right.

Mr. HOOFNAGLE. I do think it makes sense to consider using the word "misuse" rather than "harm." The word "misuse" is more relevant. It has better context in privacy law, and that "harm" is usually equated with financial loss or injury, but sometimes data are stolen, sometimes there are security breaches made that are mere misuses of information. So—

Chairman FEINSTEIN. Define "misuse."

Mr. HOOFNAGLE. A use of the data that is not compatible with its collection. Now, that is a confusing way of saying using the data in such a way that the victim would object to, and a common example would be the pretexting cases where information was used to investigate other people but not to steal their identity.

Chairman FEINSTEIN. Oh, I see where you are going.

Mr. HOOFNAGLE. Or where data are stolen to embarrass another person or, let's say, data are stolen to locate a domestic violence victim. Those type of risks are particular to certain people, and the entity that is experiencing the breach may not know about those risks.

Chairman FEINSTEIN. Well, take a data base like UCLA had of 800,000. If it were misused, how would they ever get to the point they got to? Because you would never know. All these other issues enter into it with respect to misuse.

Mr. HOOFNAGLE. Well, it would be "reasonable risk of misuse" instead of "significant risk of harm." So there is going to be a risk assessment made, and I think it makes more sense to assess whether or not the information is going to be misused, not whether or not there will be harm flowing from the incident.

Chairman FEINSTEIN. Well, we have opened a whole other chapter. Can you comment, Mr. Davis?

Mr. DAVIS. I have to think about that one.

Chairman FEINSTEIN. Yes, I do, too. I do not know what it means, really. I understand what he is saying, but in terms of a law—I mean, I know what harm is, but is it proper use? Is it misuse? And you have 800,000 people, all of whom—take the case of

UCLA. You have applicants, you have students, you have alumni. What else do you have on that data base?

Mr. DAVIS. And we had some people from the Office of the President and faculty.

Ms. MCNABB. And you?

Mr. DAVIS. I did get a letter.

[Laughter.]

Chairman FEINSTEIN. So you had a cross-section of people. Now, if you go into the private sector away from a University setting, you are going to have an even broader group of people. Let's say it is a bank that has its data breached that owns insurance companies, and all that stuff, it is millions of pieces of data. How do you determine whether misuse would occur? How do you determine even who the population is? It seems to me it is a huge delaying effort just to get to that point.

Mr. HOOFNAGLE. You are right, Madam Chair. This is the most difficult issue in security breach notification. But what I am trying to say is that we do not want entities just looking for risk of identity theft. There are other risks out there.

Chairman FEINSTEIN. Yes, but this is aimed at identity theft. It is not aimed at taking care of all the world's problems. That is the hard part of this. I see where you are going, but we have enough trouble moving this bill now.

Mr. HOOFNAGLE. Well, it would be important, for instance, if a data base were breached, if information were stolen from a business by someone who attempted to stalk another person, to locate a domestic violence victim, to embarrass that person, that would be—

Chairman FEINSTEIN. But how would the bank know? How would the insurance company know?

Mr. HOOFNAGLE. It might become apparent in the risk assessment. Of course, every situation is different. What I am saying is that the scope—

Chairman FEINSTEIN. You cannot do a risk assessment for every single person in that data base. There are millions. You have to do this in a timely way, within a very limited period of time.

Mr. HOOFNAGLE. Let's consider the pretexting scandals where individuals' records were accessed without authorization. Those were single individuals' information that was stolen. It was not done for identity theft. It was done to investigate those people and possibly to embarrass them.

What I am saying is that the scope of harms that may occur to a victim are broader, and sometimes in the risk assessment it will be possible to determine that. Sometimes it will not.

Chairman FEINSTEIN. Well, it seems to me with the word "harm" it is a much more general phrase that you identify whether this particular break is apt to result in any kind of harm to an individual whose name or data is in that data base. And if the answer is yes and it is a significant risk of harm, you have to do certain things. If the answer is no, then you submit your assessment. The Secret Service will take a look at it and either agree with you or disagree with you.

Mr. HOOFNAGLE. That is a sensible definition of "harm," and what I would recommend is that the Committee report language

specify that the harms, the possible harms, can be broader than just physical harm or identity theft.

Chairman FEINSTEIN. Well, I will think about it.

Mr. HOOFNAGLE. OK.

Chairman FEINSTEIN. How is that one?

Mr. HOOFNAGLE. That is perfect.

[Laughter.]

Chairman FEINSTEIN. Thank you all very, very much. I think it has been an interesting hearing. I very much appreciate what you do. Please stay the course and continue on, and we will as well. Thank you.

The hearing is adjourned.

[Whereupon, at 4:05 p.m., the Subcommittee was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

Written Testimony of Jim Davis
Associate Vice Chancellor, Information Technology
Chief Information Officer
Professor of Chemical Engineering
University of California, Los Angeles
Before the Subcommittee on
Terrorism, Technology and Homeland Security
Committee on the Judiciary
United States Senate

Identity Theft: Innovative Solutions for an Evolving Problem

March 21, 2007

Lessons Learned from Notification of a Large Breach

Madam Chairwoman, Ranking Member Kyl, Members of the Committee, I appreciate this opportunity to appear before the subcommittee. Last year, UCLA was the victim of a large database security breach. More than 800,000 people were notified that their Social Security numbers might have been illegally accessed. The scale and complexity of the breach amplified the tension of competing goals raised in decision-making and resulted in a number of important lessons learned about responding to an incident of such magnitude: deciding whom to notify when computer forensics are inconclusive, the logistics of a large-scale notification and how notification aligns with our high respect for individual privacy. I would like to share some of these lessons with you today.

Computer forensics uncovered evidence that significantly confirmed only a small percentage of the 800,000 individuals in our database had their Social Security numbers accessed and needed notification under California law. The campus then faced a difficult decision about whether to notify the vast remainder of potentially affected individuals in the absence of significant confirming technical evidence. We were acutely aware of the large impact our

decision would have on the individuals and on our campus. What was the campus's position on notifying these individuals?

A clear consensus quickly emerged that UCLA wanted to do the right thing, even if it caused negative repercussions for the campus. Providing possibly broader notification than was strictly legally required was part of this position. Individual privacy is a cultural and institutional value highly regarded by the University of California and we felt notification supported this value, both as events were unfolding and subsequently during discussion of the security breach with our Advisory Board on Privacy and Data Protection.

At the same time, UCLA itself felt victimized. UCLA had taken significant technical, administrative and physical security measures to protect its sensitive data, yet it still suffered this sophisticated attack. Not only did the attack potentially affect individuals in the database, but the University made extensive efforts to assess and remediate the situation, with many staff spending night and day for several weeks working to handle the breach.

The Breach

The restricted UCLA database contains certain information on all current and some former students, faculty and staff, as well as some student applicants and some parents of students or applicants who applied for financial aid. It also includes information about all current and some former employees at the University of California Office of the President and at the University of California, Merced (for which UCLA does administrative processing). In all, information for some 803,000 persons was stored in this database, including names, Social Security numbers, dates of birth, home addresses and other contact information. It did not contain drivers license, credit card or banking information.

The FBI set up a mechanism to take reports of alleged identity theft believed to be due to this breach through their Internet Crime Complaint Center. To date, UCLA has not received any information, either directly or from the FBI, to suggest that the compromised data has been used illegally.

UCLA computer system administrators first discovered the breach on November 21, 2006, when they noticed unusually high volumes of activity on a campus data server. Further investigation indicated that an attack was in progress, and security staff took the compromised system off the network and began a computer forensics investigation.

The University of California's Electronic Information Security policy includes guidelines for uniform handling and reporting of security breaches under the California law. UCLA's well-established security incident response process was invoked, and the FBI was alerted and began conducting its own investigation. Having an incident response protocol defined in advance was critical to mounting a prompt and effective response to our security breach. While we strive for a zero incident target with respect to security, we remain prepared for the worst, a position consistent with the guidebook on Protecting Personal Information just issued by the Federal Trade Commission ("Plan Ahead" is the last step of its five-step program.)

UCLA's systems were in full compliance with University of California (UC) and campus policy governing security standards and practices, but system log analysis showed that sophisticated and malicious attackers were able to exploit an undetected flaw in one of its applications. It was particularly disturbing to find that our systems were being attacked by a criminal with clear intent to collect Social Security numbers, unlike many other breaches

reported in the press and by other UC institutions where the data was not the target – e.g., missing laptops or servers compromised for illegal music and movie file sharing.

Forensic analysis continued in the days following the initial discovery. Conducted in cooperation with the FBI, this analysis revealed organization, sophistication and a multiplicity of attack modalities that were not originally evident. Because of the sophisticated nature of the attack, the hacker was able to conceal his or her activity or make it blend in with legitimate activity, allowing the illegal access to remain undetected for a little more than a year before it was discovered in November 2006.

Whom to Notify?

By campus policy, the final decision to notify and the extent of notification rests with the chief information officer. We assembled the equivalent of an outside, objective notification review team that included the chief information officer, the UCLA directors of information technology security and information technology policy, legal counsel and the director of information technology policy for the University of California system.

In our deliberations, we faced a fundamental tension between speed and accuracy in determining whom to notify during the ongoing forensic analysis. We wanted to let potentially affected individuals know as soon as possible about the breach so they could take action by placing a fraud alert or a credit freeze; however, the complexity of the forensics meant new findings occurred almost daily, and the size of the potentially affected population changed significantly with these new findings. We did not wish to alarm and inconvenience hundreds of thousands of people if there was no reason to do so, or to send out multiple potentially conflicting notices. Woven throughout our deliberations was what the California

Law About Notification in Instances of Security Breaches (California Civil Code, §1798.29) required in the absence of positive proof.

Initial results of our computer forensics indicated a relatively small population whose data could have been acquired. Subsequent results indicated the possibility of access to the full database of 800,000; however, continued analysis led us to believe the attack was targeted only on the smaller segment of the database. In our deliberations we felt a strict interpretation of the State notification law ("...shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person") would require us to notify only this smaller subset.

In the absence of positive proof about whether the vast majority of people's information had actually been acquired, we used a set of criteria articulated by the University of California in 2003 – based on the California Office of Privacy Protection's recommended practices – to help think through exactly such ambiguous situations. Among other things, we considered the duration of the exposure and indications that the attack specifically sought personal information, whether we had any definitive evidence that the information was *not* acquired, as well as the potential harm to individuals if the wrong decisions were made. (These criteria have since been expanded upon by the EDUCAUSE/Internet2 Security Task Force, as part of their Data Incident Notification Toolkit.)

Careful consideration of all factors ultimately convinced us to notify the largest group, even without a legal requirement or evidence of acquisition. Underlying this decision was an ethical responsibility to protect against potential fraud and a high regard for the privacy of

individuals. Our goal was then to rapidly reach as many of the 800,000 people in the breached database as possible.

The Logistics of Notification

The specter of identity theft raises anxiety and anger, and we did not want to compound the situation by being ill prepared to address individuals' concerns once our notification began. As with other institutions, we deemed it essential to establish a call center and Web site prior to notification. Since we also wanted to minimize delay, our strategy was to get our base communications structure in place as quickly as possible, begin the notification process and then continually make needed adjustments as we monitored results. In tandem with our deliberations about whom to notify, the incident response team, including University Communications, built an identity alert Web site with information about the breach, what individuals could do to protect themselves from identity theft and the latest news from UCLA and the FBI. We also developed critical information to provide to the staff that would be answering phone calls from affected individuals. Finally, a call with the California Office of Privacy Protection provided several thoughts, including a recommendation to inform the three credit reporting agencies about our breach and our large notification process, which we did.

Institutions we spoke with told us to expect a 3% call rate, which translated into about 25,000 calls. Immediately, making arrangements to outsource call center operations was not just on the critical path to notification, but became the critical path: we had never had to do this before, and finding a suitable call center vendor and completing a contract on an expedited basis became mission critical.

Notification began on December 12, 2006, the earliest date possible after determining the scope of the incident, setting up arrangements to communicate with 800,000 people and being prepared to handle the huge volume of anticipated telephone calls. University of California guidelines require us to employ written hard copy or email notice, or in cases where sufficient contact information is not available, substitute a notice via prominent display on the campus Web site for a period of at least 45 days.

Our notification process was a coordinated effort involving e-mail, U.S. mail, the news media and our Web site. Letters were sent by email or U.S. mail to the approximately 70% of individuals for whom we had addresses. (UCLA's policy mandates attempted notification of all affected individuals, not only California residents as required by State law.) We issued a news release, and on the same day we placed a story in the Los Angeles Times, which led to stories in print and broadcast outlets across the country and internationally. All communications pointed to our toll-free number and Web site. Our statistics demonstrate success in reaching approximately 75-80% of the affected database population.

We received 12,000 calls the first day. At its height, the call center operation included 1,600 (non-dedicated) operators at 26 locations, handling as many as 1,000 calls per hour. To date, the hotline has received almost 36,000 calls (about 4.5% of those notified) and though now scaled back, it is still accepting calls. Operators were able to confirm that a caller was in the affected database and provide basic information about fraud alerts and credit freezes, or escalate calls to a higher-level official. They were specifically instructed to use a sympathetic tone. The statistics and feedback provided by the call center vendor were reviewed at the end of each day and used to revise and fine tune our approach and the information used by operators. For example, we heard early on that some recipients read our notification letter to

mean that their identities had, in fact, already been stolen and we modified the call center responses to correct this misunderstanding.

We found three groups of callers: the largest group felt violated and anxious and wanted the connection with a live person for answers, reassurance, clarification and empathy; a much smaller group just wanted information; and something under 2% of callers were sufficiently angered or distraught that they demanded to speak with a higher-level UCLA official. Our escalation process designated an individual who had the right combination of knowledge, sympathy and ability to ensure follow-up action to provide a return call to each such caller. Of the 600 or so callers who spoke with this individual, we had five people who remained dissatisfied.

Our Web site was a vital component of the notification process. We continued to develop and add content as new information became available that would expand its capacity to inform affected individuals. For example, we had initially relied on the credit reporting agencies' Web sites for information about placing a fraud alert. However, we received reports from callers that the procedures deviated from those described on their Web sites and so we had staff call the agencies to get specific details that was then detailed on our identity alert site. To date our Web site has received almost 105,000 unique visitors, with an average of 15,000 daily visitors during the first week following our announcements.

On January 10, 2007, a second letter was sent to approximately 28,500 individuals and posted on the identity alert Web site. By this point, our forensic analysis indicated that these were the only people for whom we had significant evidence that their Social Security numbers had actually been acquired. There remained no conclusive proof of access to the rest of the database.

Lessons Learned

We offer six actions to consider in being prepared for and in responding to a breach.

1. Convene an independent and objective panel for deliberations about whom to notify. A complex technical environment required ongoing forensic investigation to understand modes of attack, presumed intent and our belief about the degree to which the hackers had the ability to carry out this intent. Faced with rapidly shifting information, the administrative panel of experts convened was key to determining compliance with applicable California law and in judging the competing factors in notifying the large majority of individuals for whom we had no conclusive proof. We continue to believe our decision was the most suitable; but notification did cause concern and inconvenience, the drawback in notifying when the risk of harm is at best unclear.

2. Make provisions for confidentiality. As the forensics investigation continued and we were still learning about the nature and extent of the attack, we were keenly aware of the need to protect our systems from further harm to the extent possible. Maintaining confidentiality during this "learning" stage was pivotal to doing so. Concerns about confidentiality were also threaded throughout our efforts to share information with others who could have benefited from our experience, in terms of information going out prematurely that would have adversely impacted the effectiveness of our notification.

3. Ensure that the call center and Web site are ready to go when notification occurs. Given the enormous volume of callers and visitors to our Web site, without these channels of information reinforcing each other, confusion and frustration levels would surely have been much higher.

4. Notify using different channels. We preferred individual notification – email and U.S. mail – but to ensure that the affected population learned of the breach, the toll-free number and

our identity alert Web site, we also used our UCLA's home page and the media. We believe all channels we used were important: email and the media for the fastest way to reach individuals and U.S. mail for a more personalized notice. We did receive callers who expressed annoyance about not having received a personal letter or email and "only" hearing about the breach through the media, but we felt our goal of awareness had been achieved. (When we heard complaints about the lack of personalization – specifically, the use of "Dear Friend" as a salutation in our first letter – we took pains to ensure that the second group of letters was personalized with the individual's name clearly shown in a windowed envelope.)

5. Offer access to solid information through different channels and keep track of how they are used. It was important to be able to give useful and accurate information, such as the specifics on how to protect oneself from identity theft, how a fraud alert works, how a credit freeze differs from a fraud alert and how to implement them. We spent effort researching this information and tested the methods ourselves. Offering this information through both the identity alert Web site and the call center was important: individuals without a computer were unable to easily access our Web site; callers who demanded escalation from an operator often did not wish to go to the Web site; and with the volume of visitors to our Web site, doubtless many who went to the Web site to get information did not have to call. Finally, all of the statistics we kept on these communications methods have helped us to understand how successful we were in notification.

6. Spend time setting up the call center function correctly. The huge preponderance of calls came in the first couple of days. We had staffed according to what we had heard from others' experiences, but even our very generous estimates were overwhelmed on the first day when we received a full third of all calls – likely due to email notices and media outreach.

However, outsourcing the call center function provided invaluable help in the form of daily reports and an ability to scale that allowed us to continually refine our responses and procedures very quickly. Finally, defining a procedure for escalation of angry callers was indispensable. We were lucky to have had an individual with a sympathetic ear, accurate knowledge, access to follow-up action and the stamina to handle these escalated – and usually emotionally difficult – calls.

A Privacy-Centered Approach

UCLA and the University of California respect individual privacy as a fundamental cultural and institutional value and have embedded strong protections for it in its policies. Though we have no desire to be in a situation where we must notify individuals that their privacy has potentially been breached, once it is clear there is such a situation, we will err on the side of notifying individuals of the affected community to help protect their privacy. In essence, notification is consistent with our view of respecting individual privacy.

Beyond empowering individuals to protect against identity theft, the 2003 California notification law accelerated and intensified our institutional efforts to protect data. A 2005 University of California report included recommendations to enhance our policies for the stewardship of data and to strengthen educational activities and technical measures to protect sensitive data required to be collected in the normal conduct of the business of the University. UCLA, along with the other UC campuses, has been actively engaged in implementing these recommendations.

We believe avoiding retention of sensitive data is the first step. Particularly since 2003, when the California law was enacted, UCLA has made tremendous effort to reduce retention of Social Security numbers for internal business practice. In light of the breach, we have

reexamined why we keep Social Security numbers and confirmed that fundamentally, we must keep them in order to provide them to external organizations such as the Internal Revenue Service and the National Student Clearinghouse. Our ability to continue reducing retention is thus relatively modest without a concomitant reduction in the external requirements for us to provide, and therefore keep, Social Security numbers – an effective partner to incident response and notification.

The scope and technical complexity of UCLA's breach has given us some insight into what actions were effective and where there are likely to be tensions over important decisions about notification. I hope that sharing these lessons will prove valuable to others.

Attachments

1. News release: UCLA Warns of Unauthorized Access to Restricted Database (December 12, 2006)
2. Notification letter to those in the database (December 12, 2006)
3. Follow-up letter (January 10, 2007)
4. Home page of http://identityalert.ucla.edu
5. News release: FBI Advises Victims of UCLA Computer Intrusion to Report Fraud to the FBI's Internet Crime Complaint Center (December 15, 2006, http://losangeles.fbi.gov/pressrel/2006/la121506.htm)
6. Determining the Threshold for Security Breach Notification, University of California, 2003. http://www.ucop.edu/irc/itsec/security_breach_notification.pdf

UCLA NEWS

www.newsroom.ucla.edu

OFFICE OF
MEDIA RELATIONS
James West
Alumni Center

Box 951431
Los Angeles, CA
90095-1431
TEL 310.825.2585
FAX 310.206-3455

Office of Media Relations, media@support.ucla.edu
(310) 825-2585

For Immediate Use
Dec. 12, 2006

UCLA Warns of Unauthorized Access to Restricted Database

UCLA is alerting approximately 800,000 people that their names and certain personal information are contained in a restricted database that was illegally and fraudulently accessed by a sophisticated computer hacker.

This database contains certain personal information about UCLA's current and some former students, faculty and staff, some student applicants and some parents of students or applicants who applied for financial aid. Approximately 3,200 of those being notified are current or former staff and faculty of the University of California, Merced, and current or former employees of the University of California Office of the President, for which UCLA does administrative processing.

In a letter being sent to affected individuals, Acting Chancellor Norman Abrams said that personal information about at least some of the individuals was obtained by the hacker but that there is no evidence that any data has been misused. The database includes names, Social Security numbers, dates of birth, home addresses and contact information. It does not include driver's license numbers or credit card or banking information.

"We take our responsibility to safeguard personal information very seriously," Abrams said. "My primary concern is to make sure this does not happen again and to provide to the people whose data is stored in the database important information on how to minimize the risk of potential identity theft and fraud."

UCLA blocked access to the Social Security numbers and the database when suspicious activity was detected on Nov. 21 and immediately activated its information technology security incident team. UCLA also notified the FBI, which is conducting an investigation.

Even though UCLA's ongoing investigation at this time indicates only that the hacker sought and obtained some of the Social Security numbers, out of an abundance of caution, the university decided to notify all 800,000 people whose names are listed in the restricted database.

"Ensuring data security is one of the most important responsibilities we have to the campus community, and in recent years we have significantly strengthened our information security practices in response to increasing attacks. In spite of our diligence, a sophisticated

-more-

2-2-2 Database Breach

hacker found and exploited a subtle vulnerability in one of hundreds of applications," said Jim Davis, UCLA's chief information officer and associate vice chancellor–Information Technology. "We deeply regret the concern and inconvenience caused by this illegal activity. We have reconstructed and protected the compromised database and launched a comprehensive review of all computer security measures to accelerate systematic enhancements that were already in progress."

UCLA began sending notification letters and e-mails on Dec. 12, as soon as possible after determining that personal data was potentially accessed and after retrieving individual contact information. The letters suggest that recipients contact credit reporting agencies and take steps to minimize the risk of potential identity theft.

To provide information and respond to queries, UCLA has established a Web site, http://www.identityalert.ucla.edu, and a toll-free call center, (877) 533-8082.

Davis said access to the restricted database was gained by a computer trespasser utilizing a software program designed to exploit an undetected software flaw, thereby bypassing all security measures. A problem was detected Nov. 21 when computer security technicians noticed an exceptionally high volume of suspicious database queries. An emergency investigation indicated that access attempts had been made since October 2005 and that the hacker specifically sought Social Security numbers, Davis said.

For the past decade, UCLA has been systematically upgrading computer security but had not yet identified the vulnerability maliciously exploited by the computer hacker. During this time, UCLA installed and strengthened firewalls and intrusion-detection systems, removed Social Security numbers from computer screens and written reports, and prohibited their storage on portable devices, among other steps.

The UCLA incident is the latest in a string of computer security breaches affecting financial institutions, universities and other large employers. State law requires notification when personal data is reasonably believed to have been acquired.

UNIVERSITY OF CALIFORNIA, LOS ANGELES **UCLA**

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

OFFICE OF THE CHANCELLOR
BOX 951405
LOS ANGELES, CALIFORNIA 90095-1405

December 12, 2006

Dear Friend,

UCLA computer administrators have discovered that a restricted campus database containing certain personal information has been illegally accessed by a sophisticated computer hacker. This database contains certain personal information about **UCLA**'s current and some former students, faculty and staff, some student applicants and some parents of students or applicants who applied for financial aid. The database also includes current and some former faculty and staff at the **University of California, Merced**, and current and some former employees of the **University of California Office of the President**, for which UCLA does administrative processing.

I regret having to inform you that your name is in the database. While we are uncertain whether your personal information was actually obtained, we know that the hacker sought and retrieved some Social Security numbers. Therefore, I want to bring this situation to your attention and urge you to take actions to minimize your potential risk of identity theft. I emphasize that we have no evidence that personal information has been misused.

The information stored on the affected database includes names and Social Security numbers, dates of birth, home addresses and contact information. It does not include driver's license numbers or credit card or banking information.

Only designated users whose jobs require working with the restricted data are given passwords to access this database. However, an unauthorized person exploited a previously undetected software flaw and fraudulently accessed the database between October 2005 and November 2006. When UCLA discovered this activity on Nov. 21, 2006, computer security staff immediately blocked all access to Social Security numbers and began an emergency investigation. While UCLA currently utilizes sophisticated information security measures to protect this database, several measures that were already under way have been accelerated.

In addition, UCLA has notified the FBI, which is conducting its own investigation. We began notifying those individuals in the affected database as soon as possible after determining that personal data was accessed and after we retrieved individual contact information.

As a precaution, I recommend that you place a fraud alert on your consumer credit file. By doing so, you let creditors know to watch for unusual or suspicious activity, such as someone attempting to open a new credit card account in your name. You may also wish to consider placing a security freeze on your accounts by writing to the credit bureaus. A security freeze means that your credit history cannot be seen by potential creditors, insurance companies or employers doing background checks unless you give consent. For details on how to take these steps, please see the attachment to this letter.

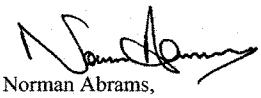
Information also is available on a Web site we have established, http://www.identityalert.ucla.edu. The site includes additional information on this situation, further suggestions for monitoring your credit and links to state and federal resources. If you have questions about this incident and its implications, you may call our toll-free number, (877) 533-8082.

Please be aware that dishonest people falsely identifying themselves as UCLA representatives might contact you and offer assistance. I want to assure you that UCLA will not contact you by phone, e-mail or any other method to ask you for personal information. I strongly urge you not to release any personal information in response to inquiries of this nature.

We have a responsibility to safeguard personal information, an obligation that we take very seriously.

I deeply regret any concern or inconvenience this incident may cause you.

Sincerely,



Norman Abrams,
Acting Chancellor

Extensive information on steps to protect against personal identity theft and fraud are on the Web site of the California Office of Privacy Protection, a division of the state Department of Consumer Affairs, http://www.privacy.ca.gov.

PLACING A FRAUD ALERT

By placing a fraud alert on your consumer credit file, you let creditors know to watch for unusual or suspicious activity in any of your accounts, such as someone trying to open a credit card account in your name.

To place a fraud alert, call one of the following three major credit reporting agencies. Your phone call will take you to an automated phone system. Be sure to listen carefully to the selections and indicate that you are at risk for credit fraud.

You need only contact one of these agencies, which will automatically forward the fraud alert to the other two.

Equifax
(888) 766-0008
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
http://www.equifax.com

Experian
(888) 397-3742
Credit Fraud Center
P.O. Box 1017
Allen, TX 75013
http://www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
http://www.tuc.com

Soon after you place a fraud alert, you will receive credit reports by mail from all three credit reporting agencies. In the credit report:

- Check your personal information, including home address, Social Security number, etc., for accuracy.
- Look for any charges you didn't make.
- Watch for any accounts you didn't open.
- Note any inquiries from creditors that you didn't initiate.

If you find anything that looks wrong or suspicious or that you don't understand, call the credit agency at the telephone number listed on your credit report. You may also wish to call your local police or sheriff's office to file a report of identity theft.

PLACING A SECURITY FREEZE

A security freeze means that your credit file cannot be shared with potential creditors. If your credit files are frozen, even someone who has your name and Social Security number would probably not be able to get credit in your name. A security freeze is free to those who have a police report of identity theft. If you don't have a police report, it costs $10 to place a freeze with each credit bureau, for a total of $30. The credit bureaus require that freeze requests be made in writing.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

- Send by certified mail.
- Include name, current and former address, Social Security number and date of birth.
- Pay by check, money order or credit card (Visa, Master Card, American Express or Discover only). Give name of credit card, account number and expiration date.

Experian Security Freeze
P. O. Box 9554
Allen, TX 75013

- Send by certified mail.
- Include full name, with middle initial and Jr./Sr., etc.
- Include current address and home addresses for past five years, Social Security number, birth date and two proofs of residence (copy of driver's license, utility bill, insurance statement, bank statement).
- Pay by check, money order or credit card. Give name of credit card, account number and expiration date.

TransUnion Security Freeze
P. O. Box 6790
Fullerton, CA 92834

- Send by regular or certified mail.
- Include first name, middle initial, last name, Jr., etc.
- Current home address and addresses for past five years, Social Security number and birth date.
- Pay by check, money order or credit card. Give name of credit card, account number and expiration date.

UNIVERSITY OF CALIFORNIA, LOS ANGELES **UCLA**

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

OFFICE OF THE CHANCELLOR
BOX 951405
LOS ANGELES, CALIFORNIA 90095-1405

January 10, 2007

Dear:

I am writing to provide you with additional information regarding the database security incident announced in December. At that time, UCLA announced that a sophisticated computer hacker illegally accessed a database containing certain personal information and that the hacker sought and obtained at least some Social Security numbers. Through our continuing investigation, we have now confirmed that the hacker retrieved approximately 28,600 Social Security numbers. These Social Security numbers related to approximately 18,500 UCLA student financial aid applicants from 2002 through 2006 and approximately 10,100 former employees who separated from UCLA, the University of California Office of the President and UC Merced between 1995 and 2003, plus one who left in 1988.

We wanted to immediately notify members of these groups that their data was accessed by the hacker. I am very sorry to report that your Social Security number was among the 28,600 illegally retrieved. This does not mean that you are the victim of identity theft or that we have evidence of your Social Security number being misused. And it is important to know that the database does not include banking or credit card information or driver's license numbers. However, I want to reiterate my previous recommendation that you take steps to protect against potential fraud.

The attachment to this letter provides information on how to place a fraud alert on your consumer credit file. By doing so, you let creditors know to watch for unusual or suspicious activity, such as someone attempting to open a new credit card account in your name. A fraud alert, which can be reinstated after the initial 90-day period, also entitles you to a free credit report from each of the three national credit bureaus. In addition to free credit reports available to those placing fraud alerts, federal law entitles consumers to one free credit report from each credit bureau once a year. By staggering the times at which free credit reports are ordered, consumers can monitor their own credit.

There are many resources available at the special Web site we have established, http://www.identityalert.ucla.edu, including links to useful sites operated by the U.S. Department of Justice, the Federal Trade Commission, the California Office of Privacy Protection, and the Identity Theft Resource Center. If you have questions about this incident and its implications, you may call our toll-free number, (877) 533-8082.

Once again, I want to express my deep regret for any concern or inconvenience this incident may cause you.

Sincerely,

Norman Abrams
Acting Chancellor

Attachment

UCLA

Identity Alert

Identity Alert Home Page

Protecting Your Credit

Additional Credit Protection Options

Frequently Asked Questions

Resources

Notification Letter (Dec.12, 2006) (text only version)

Follow-up Letter (Jan. 10, 2007) (text only version)

News Release

This Web site has been established to provide information about an incident in which a sophisticated computer hacker illegally accessed a UCLA database. The announcement was made Dec. 12, 2006, and UCLA began notifying approximately 800,000 people whose names and certain personal information are in the database (see **Notification Letter**). UCLA takes seriously its responsibility to safeguard personal information and regrets the inconvenience caused by this illegal and fraudulent activity.

Key Updates:

- An ongoing investigation has found that the Social Security numbers of approximately 28,600 people in the database were illegally retrieved by the hacker. UCLA began notifying them on Jan. 10, 2007 (see **Follow-up Letter**). The affected parties are limited to approximately 18,500 UCLA student financial aid applicants from 2002 through 2006 and 10,100 former employees who separated from UCLA, the University of California Office of the President and UC Merced between 1995 and 2003, plus one who left in 1988. If you are in this group, it does not mean you are the victim of identity theft or that your Social Security number has been misused.

- If you want to know whether you are among the approximately 800,000 people in the database or among the 28,600 whose Social Security numbers were illegally retrieved by the hacker, call the Identity Alert Hotline established by UCLA. The phone number is (877) 533-8082. Operators may need to ask you for additional information, such as the month and day of your birth or the last four digits of your Social Security number, in order to distinguish you from others with the same name.

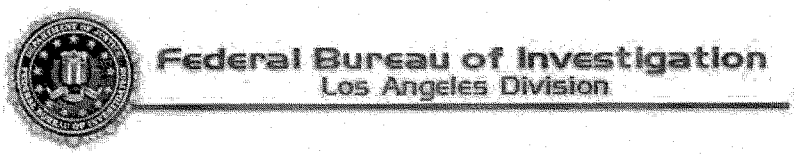
- Regardless of whether or not the hacker has your personal information, UCLA recommends that all those in the compromised database contact the three national credit bureaus to place a fraud alert on their credit files. This instructs creditors to watch for unusual or suspicious activity, such as someone attempting to open a new credit card account in your name. A fraud alert, which can be reinstated after the initial 90-day period, entitles consumers to a free credit report from each of the three national credit bureaus. In addition to free credit reports available to those placing fraud alerts, federal law entitles consumers to one free credit report from each credit bureau once a year. By staggering the times at which free credit reports are ordered, consumers can monitor their own credit without incurring financial costs. Details on protecting your credit are available on this site at **Protecting Your Credit** and **Additional Credit Protection Options**.

- If you believe you are a victim of fraud or identity theft resulting from this hacking incident, UCLA and the FBI urge you to contact the FBI's Internet Crime Complaint Center and submit an online report. In a news

release, the FBI said: "All reports submitted will be analyzed and follow-up action taken where appropriate."

Reports can be filed at: **http://www.ic3.gov.**
The news release is at:
http://losangeles.fbi.gov/pressrel/2006/la121506.htm.

If you do not have Adobe Reader installed, you can down a free copy by clicking the red button to the left.



FBI * 11000 Wilshire Blvd. * Los Angeles, Ca 90024 * 310-996-3804,3343,4402 * Fax: 310-996-3345

For Immediate Release

DATE: December 15, 2006

FBI Advises Victims of UCLA Computer Intrusion to Report Fraud to the FBI's Internet Crime Complaint Center

On December 12, 2006, UCLA alerted approximately 800,000 individuals that their names and certain personal information contained in a restricted database had been illegally accessed by a sophisticated computer hacker. This database contained certain personal information, including Social Security numbers, dates of birth and home addresses, regarding current and some former UCLA students, faculty and staff, some student applicants and some parents of students or applicants who had applied for financial aid.

The FBI has initiated an investigation into the illegal access of the computer network at UCLA to determine those responsible, the extent of the computer intrusion and potential related criminal activity.

The FBI is urging anyone who was notified by UCLA that their information has been compromised and who believe they may have been victimized further by identity theft or by other fraudulent means to contact the FBI's Internet Crime Complaint Center and submit an online report. Individuals submitting reports should clearly indicate the nature of their affiliation with UCLA including their department, major, position, the month and year of their initial affiliation with UCLA and, if applicable, the date that affiliation ended. The reports should also include information as to whether or not the complainant has had his/her identity stolen or has been the victim of other identity-related fraud since June 2005. All reports submitted will be analyzed and follow-up action taken where appropriate.

The above reports should be submitted to the FBI's Internet Crime Complaint Center at: www.ic3.gov.

UCLA will also place a link to the FBI's Internet Crime Complaint Center at www.ic3.gov on the website they have set up in connection with this matter.

University of California Office of the President
Information Resources and Communications

Determining the Threshold for Security Breach Notification

November 25, 2003

Background

California law requires notification to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a security breach. No criteria for reasonable belief are provided in the statute. The University of California Business and Finance Bulletin IS-3 Electronic Information Resources Section IV.D identifies requirements for University of California compliance with this statute. Section IV.A, which addresses data sensitivity, requires that campuses implement procedures to provide physical and logical security of this information.

Deciding Whether or Not to Notify

Campuses should consider the factors listed below in making a determination to notify for any security incidents subject to this regulation.

The Office of Privacy Protection in the California Department of Consumer Affairs http://www.privacy.ca.gov/recommendations/recomend.htm recommends that the following factors be considered when making a determination to notify:

Acquisition

In determining whether unencrypted notice-triggering information has been *acquired*, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:

1. Indications that the information is *in the physical possession and control* of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
2. Indications that the information has been *downloaded* or copied, for example: an ftp log that contains the name of a file containing notice triggering information.
3. Indications that the information was *used* by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(See: http://www.privacy.ca.gov/recommendations/secbreach.pdf)

The University of California recommends consideration of these additional factors:

- Duration of exposure.
- Indications that *any* download or copy activity has occurred, even if there is no specific evidence that there was a download or copy of data subject to the law.
- The extent to which the compromise indicates a directed attack, such as a pattern showing the machine itself was specifically targeted.
- Indication that the attack intended to seek and collect personal information.

Campuses may use additional criteria to determine whether to notify.

Campuses should feel free to contact campus counsel at any step of the process if they have questions or want legal consultation.

Other Considerations

In addition to the factors listed above, there may be other circumstances to be considered when deciding whether or not to abide strictly by the requirements imposed by the law. As an example, although the law doesn't apply to data that is encrypted, if encrypted information is reasonably believed to have been acquired as a result of a security breach, the extent to which the encryption method would prevent the information from being used should be considered when deciding whether or not to notify.

The law states: "Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure." However, notification would be required if an employee misuses authorized access to disclose personal information. Note as well that an employee disclosing previously encrypted personal information on an unauthorized basis would trigger notification.

If there is difficulty reaching a decision whether or not there is a reasonable belief that data may have been acquired as defined by this law, campuses may also consider the potential damage to individuals if the wrong decision is made. For example, one should weigh the potential for identity theft or financial abuse if it turns out that the data had been acquired and no notice was sent.

STATEMENT OF EDWARD M. KENNEDY
Hearing on "Identity Theft: Innovative Solutions for an Evolving Problem"
Senate Judiciary Committee
March 21, 2007

American citizens are becoming victims of identity theft at an alarming rate. Last year, nearly 9 million Americans had some part of their identity stolen. Victims spent 300 million hours attempting to clear their names and re-establish good credit ratings, at a cost to the economy of $56 billion dollars.

Those numbers are shameful enough. But these are only the tip of the iceberg, because they refer only to cases where lost or stolen data was fraudulently used. A vast amount of personal data is no longer secure and is waiting to be used by criminals. Estimates suggest that since February 2005, the total number of lost or exposed personal records exceeded 100 million. Not all of this information was used by criminals, but the problem is obviously escalating, and it deserves a stronger federal response.

It's become too easy for potentially harmful personal data to become public. The increasing levels of identity theft are largely a product of technology and the information age. Criminals can obtain information such as Social Security numbers, bank accounts, credit card numbers, drivers' license numbers, and medical and student records by hacking into corporate, government, academic, and personal computers. Not all personal information, however, is stolen by hackers. Often, careless business practices and personal practices lead to the information becoming publicly available. In a recent example, 26 million veterans and their spouses became vulnerable to identity theft when a Veterans Affair data analyst took home a laptop computer containing personal data which was later stolen in a burglary.

The consequences of such security breaches can't be underestimated. When an individual's personal information becomes publicly available, the damage is permanent because names, social security numbers, and dates of birth do not change. A criminal can use such information to obtain a credit card, work papers, or even a home with an innocent person's identity. More must be done to curb these attacks.

Technology has created a world in which a few key strokes can lead to the theft of a person's finances, security, and identity. The federal government has a duty to combat this epidemic, and do so responsibly. We need comprehensive legislation that does not impose insurmountable administrative burdens, but does ensure that victims of identity theft have notice of any breaches and have adequate remedies when these serious crimes occur.

Statement of Senator Patrick Leahy,
Chairman, Committee on the Judiciary,
for Subcommittee on Terrorism, Technology and Homeland
Security, Hearing on "*Identity Theft: Innovative Solutions for an Evolving Problem*"
March 21, 2007

I commend Senator Feinstein for conducting today's subcommittee hearing on "*Identity Theft: Innovative Solutions for an Evolving Problem.*" The evolving problem of identity theft remains a serious threat to Americans' privacy and it is an issue that the Judiciary Committee should carefully examine.

According to the Privacy Rights Clearinghouse, more than 100 million records containing sensitive personal information -- such as name, address and social security numbers -- have been involved in data security breaches since 2005. Despite this sobering statistic, we continue to learn about more and more data breaches that expose millions of Americans to identity theft.

Earlier this year, mega-retailer TJX Companies, Inc. disclosed that it suffered a major computer breach involving the credit and debit card purchases of hundreds of thousands of American consumers. The scope of the damage to Americans' privacy resulting from this breach remains unknown, but many believe that this breach has put thousands of U.S. consumers at risk of identity theft.

These data security breaches are compelling examples of why we need strong federal data privacy and security laws to help prevent identity theft. Last month, Senator Specter and I reintroduced our *Personal Data Privacy and Security Act*, S. 495, a comprehensive data privacy bill to protect Americans' sensitive personal information. While Senator Specter and I certainly do not have a monopoly on good ideas to solve the serious problems of identity theft and lax data security, we have put forth some very meaningful solutions to this problem in this bill. I hope that the Senate will pass this bill this year.

Today, Americans live in a world where, with just a few keystrokes on a computer, their most sensitive personal information can be accessed and sold to the highest bidder. Yet, our privacy laws lag behind the capabilities both of today's technology and the cunning of identity thieves. This is an important issue for this Committee to examine and I look forward to exploring ideas about how to best address the problem of identity theft.

####

United States Senate Committee on the Judiciary
Subcommittee on Terrorism, Technology & Homeland Security

Identity Theft: Innovative Solutions for an Evolving Problem
March 21, 2007

Testimony of
Joanne McNabb, Chief
California Office of Privacy Protection

Chairman Feinstein, distinguished members of the Subcommittee, thank you for the opportunity to share with you California's experience over the past several years in tackling identity theft. My name is Joanne McNabb and I am Chief of the California Office of Privacy Protection. The Office of Privacy Protection, in existence since 2001, is an education and advocacy office, with a mission of identifying consumer problems in the privacy area and facilitating the development of fair information practices. The Office's functions include assisting consumers with privacy concerns; providing information and education to consumers and to organizations; coordinating with law enforcement on identity theft and other privacy crimes; and recommending privacy practices to organizations.

From the beginning, identity theft has been the focus of many of our efforts. Historically over 60% of the calls and email we get are about identity theft. Several of the consumer information sheets available on our Web site cover aspects of identity theft and most of our Recommended Practices documents for businesses and other organizations address the responsible handling of the personal information that is the target of identity thieves. Last year we conducted or participated in 50 consumer workshops and seminars on identity theft, including 19 last June for veterans and military personnel in collaboration with the California Department of Veterans Affairs, and also 41 seminars on privacy practices for business or government.

California has been acknowledged as a national leader in privacy protection and in responding to identity theft. Since 1999, the California Legislature has enacted more than 80 privacy laws, 31 of them on identity theft. The Schwarzenegger Administration has made identity theft a priority, increasing the budget of the Office of Privacy Protection to enable us to undertake a program that has included developing a law enforcement manual on identity theft investigation and prosecution, working with universities on privacy and security awareness, training community-based organizations in identity theft victim assistance and prevention strategies, and developing privacy training materials for all State employees. This April we will hold our third annual California Identity Theft Summit. The first Summit, in 2005, focused on identifying the barriers to the investigation and prosecution of identity theft crimes. The 2006 Summit responded to some of the findings of the previous year by providing targeted training for all those who

must play a role in stemming this crime – consumers, business, law enforcement officers, prosecutors, and government. This year's Summit, "Protecting Privacy Online," will include more training sessions and also policy discussions of two issues critical to preventing identity theft: privacy and public records, and verifying identity in the online world.

California laws intended to prevent or respond to identity theft have served as models for other states and for the federal government. The 2003 FACT Act amendments to the Fair Credit Reporting Act contained several provisions based on California laws, including the truncation of credit card numbers on customer receipts, the requirement to securely destroy certain customer records, and the rights of identity theft victims to block fraud-related items in credit files and to get copies of documents on fraudulent accounts. California laws such as those on notice of security breach, freezing credit files, and the confidentiality of Social Security numbers have inspired many states to enact similar laws and are, as we know, being considered in Congress.

Because California has had these laws in effect for a few years now, I would like to share with the Subcommittee some of the observations of the California Office of Privacy Protection on the impact they seem to be having. I base these comments on what we learn in advising consumers of their rights and recommending strategies to pursue them, and in discussing information-management practices with businesses and other organizations.

Social Security Number Confidentiality

I want to highlight the measures that seem to be having an impact on protecting consumers and protecting personal information. The first is a law that took effect starting in 2003, prohibiting the public posting or display of Social Security numbers. We all know that Social Security numbers have become the key to the vault for identity thieves, giving them the ability to open new credit accounts, get medical care, gain employment, even create criminal records in victims' names. The California law does not prevent organizations from using Social Security numbers for internal administrative purposes, but instead focuses on making the numbers less publicly available. It is thanks to this law, for example, that my Blue Shield card no longer has my Social Security number on it. It's also why colleges and universities in California no longer use Social Security numbers on student ID cards, thereby removing the number from many other uses as well: every professor no longer has to have every student's Social Security number on class lists. The presence of Social Security numbers on public records that end up on the Internet remains a challenging problem, involving the potentially competing values of open government and individual privacy.

Security Breach Notification

Certainly the best known California privacy law is the one requiring businesses and state agencies to notify individuals of a security breach involving their personal information. Taking effect in mid-2003, the law defines personal information narrowly, as the kind that identity thieves are after: name plus Social Security number, driver's license or state ID number, or financial account number. When the law was being considered by the California Legislature it was discussed as a way to give individuals early warning that a

breach may have put them at risk of identity theft, thereby allowing them to take steps to protect themselves. Much of the debate on such laws has focused on how to define a notification trigger based on an appropriate level of risk. The California law was conceived as risk-triggered, based on the assumption that acquisition of the information by an unauthorized person – or the reasonable belief in such acquisition – constitutes a risk.

The California Office of Privacy Protection does not enforce the breach notice law, or any other privacy law. Our role in dealing with breaches has been to assist both notice recipients and organizations that experience breaches. We are part of our state government's breach response procedure, and we also have regular conversations with other organizations experiencing breaches. We first issued our "Recommended Practices on Notice of Security Breach" when the law took effect. It contains best practice recommendations on prevention, preparation for notification, and notification. The recommendations are based on fair information practice principles and input from an advisory group of stakeholders, updated with what we've learned from breach notification incidents over the past four years.

While the original intent of the law may have been to warn individuals of potential identity theft, and the law has had that result, I think the larger impact has been on improving the information management practices of organizations. Whereas information security has generally been viewed by organizations as a cost only, the requirement to notify has revealed the cost of insecurity. A 2006 benchmark study by the Ponemon Institute found that the cost per individual notified was $187. For many organizations, that cost, which includes lost business, justifies spending on security measures to protect information.

I would like to summarize some of the lessons that have been learned – or in same cases are still being learned – from breaches.

The Office of Privacy Protection learns of breaches in several ways. Individuals who have received notices call or e-mail us. State agencies consult with us as part of their incident response procedure. Occasionally companies call us, sometimes anonymously, when considering a possible notification. And, like everyone else, we learn about incidents through the news media. We have reviewed available information on 530 breach notifications since 2003. Our set does not contain every breach notification that has occurred, but it probably contains nearly all of those that affected enough people to attract media attention.

When we learn of a breach from a notice recipient, we generally contact the organization's privacy or compliance office. We may ask for more information or a copy of the notice, to help us in responding to consumer callers. We let the organization know of the assistance we can provide. Our Recommended Practices document contains sample notice letters, covering the different types of personal information that may be involved. We have a one-page flyer, in English and Spanish, which explains simply what steps an individual should take in response to a breach involving Social Security numbers only.

We also have Frequently Asked Questions for call centers, which cover the typical questions people ask, mostly about dealing with credit bureaus. All of these are available on our Web site.

What Types of Organizations Are Notifying of Breaches?

In our sample of 530 breach notifications, universities and government agencies account for most of the incidents, about 28% universities and 25% government. The prominence of universities may be explained by a couple of factors that create special challenges for information security on campus. The culture encourages the free flow of information as part of academic freedom and the scientific method. Campuses usually have very decentralized information technology structures, with individual departments, schools, centers and programs operating their own systems, making system-wide policies and procedures difficult to enforce. I also think that universities might be particularly responsible about reporting and notifying of breaches.

Financial services companies experienced 14% of the breaches in our set, medical facilities 11%, retailers 5%, and schools 3%. The remaining 15% are manufacturers, data brokers, and other businesses.

What Types of Breaches Are Triggering Notification?

Nearly half (46%) of the notifications in our sample are the result of lost or stolen laptops and other devices. Hacking, which was the nature of the breach that led to the passage of the California law, accounts for 21%. Web site exposures make up 11%, insider theft 5%, improper disposal 5%, mis-sent mail 3%, mis-sent email 2%, lost shipments or mail 1%, outsider fraud 1%, and other 3%. (It is worth noting that breaches resulting from mailing errors involved paper records, arguably not "computerized data," but some companies have taken a best practices approach and notified even when the law's application is not clear.)

Social Security numbers, the most problematic type of personal information, were involved in 69% of the breaches. Financial account numbers, including credit card numbers, were at risk in 17%, and driver's license numbers in 4%. In 18%, either other types of personal information, such as passport numbers, were involved or we don't know what information was involved. (The numbers add to more than 100% because some incidents involved more than one type of information.)

What Have We Learned from Breaches?

One lesson – made clear by the significant share of breaches resulting from lost or stolen devices – is that organizations need to pay more attention to how they protect personal information when it's on a portable computer or other device. Some organizations are doing this by using encryption on laptops and other portable devices. California state government policy requires agencies to encrypt personal or confidential information on laptops and other portable devices. Some organizations have adopted new procedures to safeguard the information, such as cabling PCs to desks or not allowing the downloading of Social Security numbers from mainframes onto PCs or laptops. Some have tightly restricted the number of people who are permitted to carry sensitive personal information on portable devices.

Another lesson, which should not come as a surprise, is the ubiquity of Social Security numbers in databases and other records. Fully 69% of the breaches in our sample involved Social Security numbers. Individuals face the greatest risk of serious identity theft problems when their Social Security numbers fall into the wrong hands. With a name and a Social Security number, an identity thief can open new credit accounts, take out a car or mortgage loan, gain employment, claim government benefits or even create a criminal record. Recovering from these types of identity theft can take hundreds of hours and thousands of dollars, making early discovery critical.

Some organizations that have experienced breaches of Social Security numbers have revised their data retention policies. After a breach that exposed 15-year-old data, a university decided not to retain certain information, including Social Security numbers, on applicants who were not admitted.

Others have reconsidered their collection of the sensitive personal information in the first place. One blood bank which, like several others with mobile operations, had a laptop stolen, changed its policy of collecting Social Security numbers and decided to rely instead on the unique donor numbers that they were already using.

Another key lesson is the need for training on privacy and security practices. It is not just information technology or human relations staff who handle personal information. On the contrary, nearly everyone in an organization – from the janitor, to the mailroom clerk, to the CEO – is likely to touch personal information on the job. The best technology and procedures can be ineffective if people do not use them properly. Training in proper information handling is a continuous process, part of building a culture that respects privacy and protects people by protecting personal information.

Security Freeze

Another California law created what is probably the strongest protection available to consumers to protect them from new-account identity theft, one of the more difficult kinds to recover from. The law giving California consumers the right to "freeze" their credit files took effect in mid-2002. It allows identity theft victims in possession of a police report to freeze their files for free and allows any individual to place a freeze for a charge of up to $10 per credit reporting agency. When a consumer has frozen her files, a credit issuer checking her credit history will receive a message saying "file frozen." This essentially prevents the issuance of new credit, because the credit issuer cannot get a credit score. The consumer receives a PIN that allows her to temporarily "lift" the freeze when she wants to apply for new credit. A freeze does not interfere with existing accounts, as existing creditors are still permitted to access a frozen credit file to perform periodic account reviews. Nor would a freeze allow someone to hide debts, since debt collectors have access to frozen files.

Since the law took effect in 2002, the California Office of Privacy Protection has received a few complaints from consumers or businesses about the functioning of a freeze. The most common complaint has been from consumers who were attempting to place a freeze and were not able to complete the process with one of the credit bureaus. In all such cases, we were able to contact the credit bureau and facilitate the process for the consumer. We have also received complaints from consumers who felt that the freeze should be available for free to all, that consumers should automatically have control of access to their credit histories.

We do not know how many Californians have frozen their credit files in the past five years. Only the credit bureaus know that. About six months after the law took effect, I understand that there were only about 150 people who had placed freezes on their files. By early 2005, soon after the ChoicePoint and other high-profile security breaches began to raise awareness of the security freeze as a protective measure, I heard that there were 4,000 California freezes. More recently, I have heard the figure quoted as 50,000. While that is a very small percentage of Californians, I think the increase demonstrates that when people learn about the option of freezing their files, many choose to do so. It is not easy for individuals to find out about the freeze, as it is not advertised in mass media and only in recent months have the credit bureaus made information about the freeze easier to find on their Web sites and automated phone systems. The number of calls the Office of Privacy Protection received from people asking how to place a freeze increased 10-fold between July 2004 and July 2005, a growth I would attribute to the mention of the freeze in news stories on breaches.

Even with much greater awareness, I would not expect the security freeze to be used by a large percentage of consumers. Unlike the Do Not Call Registry, the freeze is not free. The $10 charge per credit bureau, which comes to a total of $60 for a married couple in our community property state, is a definite barrier. It is also more difficult to place a freeze than to sign up for the Do Not Call Registry. The freeze must be requested in writing to each of the bureaus, along with a lot of personal information. Also, people who are very active in the credit market would likely find the freeze an inconvenience. It effectively moves you from the world of instant credit at the check stand to credit in three business days. For some people, waiting three days is well worth the protection afforded by a freeze.

A definition of information privacy is the ability to control one's personal information, and a security freeze allows individuals who want it to have significant control over access to the personal information in their credit files.

Criminal Identity Theft Registry

Perhaps the most difficult form of identity theft to deal with, and fortunately one of the least common kinds, is criminal identity theft. While all identity theft is a crime in California law, the term "criminal identity theft" is used to refer to an imposter's use of someone's personal information when arrested or charged with a crime, thereby creating a false criminal record for the victim. The victim of this kind of crime may lose his driver's license, be arrested repeatedly, or be unable to get work, sometimes for years.

California's approach to helping criminal identity theft victims was the creation, in 2001, of a Criminal Identity Theft Registry maintained by the California Department of Justice. Victims listed in the Registry are given a PIN and a toll-free number, which allows the victim to exonerate himself in future situations. For example, if a victim in the Registry is stopped on the highway for a broken taillight, he can tell the officer that he is a criminal identity theft victim and that a record of that status is kept in the Registry. The victim can give the officer the phone number and his PIN, allowing the officer to verify his status – a "get-out-of-jail faster" procedure. For employment situations, the Registry staff will send a letter to a prospective employer.

In order to become listed in the Registry, someone who has learned that he is a victim of criminal identity theft must obtain verification by a court, usually via a Judicial Finding of Factual Innocence. With that court order, the victim files an application to the Registry, along with LiveScan fingerprinting.

One challenge for victims has been in getting the court order. For the first four years of the Registry's existence, there were fewer than five registrants. Victims who contacted us found that they needed the help of an attorney to get the court order. In 2003, the Office of Privacy Protection developed a guide to help victims of criminal identity theft get a Judicial Finding of Factual Innocence in order to get into the Registry, making it easier for them to represent themselves. Since that time, the number of victims taking advantage of the Registry has increased to 70. With continuing education of court clerks, judges, prosecutors, and law enforcement on the procedures, we believe that the Registry represents a reasonable approach to helping victims resolve the recurring problems created by this form of identity theft.

Thank you for this opportunity to testify and to share some of California's experiences in dealing with identity theft.

Testimony and Statement for the Record of

Professor Deirdre K. Mulligan
Clinical Professor of Law;
Director, Samuelson Law, Technology & Public Policy Clinic
Faculty Director, Berkeley Center for Law and Technology
Director, Clinical Program

&

Chris Jay Hoofnagle
Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic
Senior Fellow, Berkeley Center for Law and Technology

Boalt Hall School of Law
UC-Berkeley
396 Simon Hall
Berkeley, CA 94720

Hearing on
Identity Theft: Innovative Solutions for an Evolving Problem

Before the Senate Judiciary Committee
Subcommittee on Terrorism, Technology and Homeland Security
Chairwoman Feinstein Presiding

March 21, 2007
2:30 PM
Dirksen-226

Introduction

Chairwoman Feinstein, Ranking Member Kyl, and Members of the Subcommittee, thank you for providing the opportunity to participate in this timely and important hearing. I am senior staff attorney to the Samuelson Law, Technology & Public Policy Clinic, based at Boalt Hall School of Law (University of California-Berkeley). Joining me in this testimony is Professor Deirdre K. Mulligan, who directs both the Samuelson Clinic and the Center for Clinical Education at Boalt Hall. Professor Mulligan played a key role in the conception and drafting of California Assembly Bill 700 when then Assemblyman Joseph Simitian, which was enacted by the State's legislature as SB 1386.

The Samuelson Clinic gives students hands-on training while providing a new voice for the public interest. Through the clinic, students file friend-of-the-court briefs, comment on proposed legislation and regulations, and provide legal assistance in matters that raise important issues relating to law and technology. The clinic represents consumer interests in intellectual property, communications regulation and privacy issues.

Professor Mulligan is a member of the Team for Research in Ubiquitous Secure Technology (TRUST), a multi-disciplinary, multi-institutional research project funded by the National Science Foundation. TRUST is devoted to the development of new science and technology that will transform the ability of organizations to design, build, and operate trustworthy information systems. As part of its research, TRUST is developing improved technology to combat phishing, spyware, botnets, and related threats, and studying the policy and legal context and implications of related activities such as ID theft. TRUST researchers have developed anti-phishing technologies, explored enhanced

web authentication methods, studied human factors in the installation of spyware, and researched the growing problem of botnet attacks on the internet. The full scope of TRUST's research is available online at http://www.truststc.org/. Students and staff of the Clinic and PhD and post-docs working with Professor Mulligan participate in research and policy development related to TRUST's agenda.

In our testimony today, we make recommendations on how to address the evolving problem of identity theft, including a proposal to require banks to report on identity theft incidents, and credit freezes; explain the often overlooked policy goals and benefits of security breach notification laws; provide feedback on S. 239, the Notification of Risk to Personal Data Act of 2007 and S. 495, the Personal Data Privacy and Security Act of 2007.

Overview

Congress should consider the broad policy goals of security breach notification laws. These laws are "light-weight regulatory mechanisms," modeled upon groundbreaking environmental statutes that require public reporting of releases of toxic chemicals. Like their environmental analogues, security breach notification laws create strong incentives for investment in best practices. They create incentives to reduce reliance upon sensitive personal information, particularly the Social Security number. And, they have identified areas where more security investment is needed, most immediately in the securing of laptop computers.

Research should inform policy on security breach notification. We are performing several empirical studies into aspects of security breaches. These include

research into how entities are giving notices under the current state laws, and a study into how security breach notification laws have affected security investment.

Central, standardized reporting of breaches, similar to the form of reporting required by toxic chemical release statutes would improve the effect of security breach notification efforts, by creating a centralized base of knowledge about security risks and failures that will facilitate the identification of areas ripe for best practices (whether industry driven or regulatory), identify long-hanging fruit for immediate resolution through the deployment of existing technology, practices and policies, facilitate risk assessment critical to the development of internal policies as well as external risk mitigation systems such as insurance markets, and support research to further enhance our capacity to develop secure trustworthy information systems. That is, security breaches should be registered with a federal agency and statistical information about these incidents should be made available to the public by default. Access to basic information about who has experienced breaches and how the breaches occurred will provide important guidance about how to improve the information security landscape.

The security breach notification laws around the country are laying the groundwork for a data-driven analysis of possible improvements in information and network security. Advances in the policy and technological solutions to identity theft, similarly, depend upon the availability of valid data. This data is lacking, and the policy discussion is weakened by its absence. Currently, identity theft is measured through survey polls of victims that cannot fully capture the scope of the problem. If lending institutions themselves were to report on the prevalence and severity of identity theft, a more complete picture of the problem could emerge, and adequate resources and policies

could be allocated to fighting the crime. Reporting could also create a market for identity theft safety, where banks compete to provide the products most impervious to the crime.

Credit freezes, also known as security freezes, represent an important state innovation in fighting identity theft. Because lending institutions ignore fraud alerts too frequently, credit freezes are the only remedy individuals can effectively use to prevent identity theft in certain situations. Individuals should be able to enjoy the benefits of security freezes as no cost, and be able to "thaw" their credit file quickly in order to take advantage of opportunities.

Security Breach Notification

Regulatory interventions, such as the requirement to notify individuals of security breaches, play an important role in shaping institutions' policies. The duty to give individuals notice of security breaches is similar to public reporting duties embodied in the Emergency Planning and Community Right-to-Know Act of 1986 ("EPCRA").[1] That law requires companies to make inventories of certain toxic chemicals, and to report to the public when such chemicals are released. EPCRA is reported to have a dramatic effect in reducing the prevalence of toxic releases. We make several observations on how EPCRA created a "race to the top" and how security breach notification laws have created similar incentives to improve practices:

First, just as EPCRA created strong incentives to secure toxic chemicals, security breach laws create incentives for information security investment. Prior to enactment of these laws on the state level, businesses were free to keep security incidences secret, and in effect, pass the costs to individuals who would be subject to identity theft and other

[1] 42 USC § 11023 (2007).

misuse of their data. The 2002 Computer Science and Telecommunications Board (CSTB) report on cyber security[2] noted several barriers to adequate investment in security:

- Security is expensive and is not productive,[3] which creates an incentive to invest as little as possible in security.
- Security is hard to measure, breaches are difficult to notice, and, as a result, might go unreported.
- Security has an "arms race" quality of action and reaction.
- It is easier to attack a system than it is to defend; a system might have many vulnerabilities, any one of which might be a single point of failure.
- Policymakers and researchers face a particularly acute problem of having insufficient data about information system security vulnerabilities.
- Security is an externality.[4]

The research literature on security identifies the need for a scheme to encourage investments in trustworthiness, because there is a gap between the self-interests of businesses (namely, not to invest in trustworthiness) and what's best for society (namely, trustworthy systems). Traditionally, such gaps are bridged by law and government

---

[2] National Research Council (CSTB), *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*.

[3] By this I mean that security investments do not directly contribute to individual or business productivity. I cannot use anti-virus software to write law review articles, though virus protection lowers the risk that I'll have to spend time and money recovering from a computer virus.

[4] According to Camp and Wolfram, "[e]conomists define externalities as instances where an individual or firm's actions have economic consequences for others for which there is no compensation." Compensation, of course could flow to or from the actor, leading to the distinction between *positive* (uncompensated benefits to others) and *negative* (uncompensated costs imposed on others) externalities. Economists also define a third externality, the *network externality*, which describes "products for which the utility that a user consumption of the good increases with the number of other agents consuming the good." Michael Katz and Carl Shapiro, *Technology Adoption in the Presence of Network Externalities*, 94 J. Pol. Econ. 822 (1986).

regulation. Thus, the question is what legal rules might be effective in altering investments. Security breach notification laws have caused entities to internalize more of the costs of the use and misuse of personal information, by responding to some of the failings noted by the CSTB.

Second, information disclosure and reporting mechanisms can encourage companies to reduce the risk to the public of a harm, without directing the business to take specific actions. Whereas typically, regulation places government in the midst of business practices to specify standards and procedures, these light-weight mechanisms leave businesses with more leeway for finding solutions. The mechanism ensures compliance through transparency, using "sunlight as a disinfectant." They also mitigate a key objection to regulation, in that they do not reify a given set of best practices but rather encourage those in the best position to evaluate new threats and risks to invest wisely in technologies, practices and policies to secure assets and information.

In the context of security breach notification laws, as part of the internalization of costs, entities have much stronger incentives to reduce the collection of sensitive personally identifiable information, particularly the Social Security number. Because the Social Security number plays a key role in identification and authentication in the credit markets, it is important that information policy discourage its collection and use.

Third, in the EPCRA context, disclosure of toxic releases provided benchmarks and information that could inform where additional investment was needed. The same is true in the security breach notification context. These laws have identified areas where more security investment is needed. For instance, based on news reports and statements issued by entities that have experienced breaches, we know that laptop theft is a major

vector for data loss. Investments can now be tailored to that specific vector, and we believe we will see new products developed to ensure that data on laptops are more secure from theft. We know that the economic calculus around investment in encrypting data on portable devices has been altered due to security breaches that have been disclosed.

Accordingly, like the EPCRA before it, security breach laws perform more functions than simply warning individuals of risk. As such, focusing only on identity theft is a narrow view of the benefits of security breach notification laws. These laws have contributed to security investment, changes in the collection of personal information, and a better understanding of security risks.

In our research, we are interviewing Chief Security Officers to understand the effect of the security breach disclosure laws on their role in the institution and the institutions behavior and investments around information and network security. We have also collected 206 security breach notification letters. We are coding the letters for over thirty variables to learn more about breaches and how companies choose to give notice. For instance, we are trying to determine how long entities take to provide notice after experiencing a breach, what vulnerabilities cause breaches, whether entities typically offer credit monitoring or other remedial efforts, and whether basic letter writing forms are followed (i.e. whether a date appears on the letter, whether contact information for the entity experiencing the breach is provided, and so on). When we have completed coding the information, we will share our report and raw statistics with the Committee and the public.

Security Breach Notification: State Law Innovations

As part of our research, we have surveyed the various state laws that require notification of security breaches. Several states have created new innovative approaches to the problem. These innovations should be considered in any federal legislation; some should be adopted.

First, several states, including New York, New Jersey, and North Carolina, require some form of centralized reporting after a breach. This is an important innovation that should be adopted at the federal level. There are cases where a breach affects a single individual. These breaches may be a result of exceptionally poor practices, but are unlikely to come to public light if small numbers of individuals are told of them. Centralized reporting will allow consumer protection authorities to track trends in security breaches, large and small, and to determine whether entities are providing adequate protections for information.

Second, both New York and North Carolina officials have developed standard forms for reporting breaches. These forms are attached as Appendix A. A version of them should be adopted at the federal level. Having a standard form encourages entities to disclose basic information about breaches, such as the date that the breach occurred, how it occurred, and how many people were affected. In our coding of security breach letters, we have already found that this basic information is omitted in some cases. Reporting also allows for the statistical study of breaches, which in turn, can inform information security policy and investment.

Similar form reporting under the EPCRA has enabled citizens to use toxic release data for civic engagement and research. Benchmarking and information analysis will be possible if form reporting is mandated for security breaches.

Finally, states have created new personal information triggers for security breaches. Some protect medical information, and the account numbers of savings and checking accounts, account passwords, and biometric identifiers.

S. 239, The Notification of Risk to Personal Data Act of 2007

Senate Bill 239, the Notification of Risk to Personal Data Act of 2007, is an ambitious proposal that will require both businesses and federal government agencies to give notice of some information security breaches. The legislation is broader than many state mandates, in that it covers a wider array of companies that possess but do not own personal information. For instance, a company that processes data for others that experiences a breach may not have to give notice under state laws, as it neither owns nor licenses the data. S. 239 would fix this loophole.

It defines security breaches broadly, but only requires notice of breaches involving "sensitive personally identifiable information." Nevertheless, many identifiers can serve as a trigger for issuing a breach notice. For instance, biometric data, account numbers, and combinations of home address, date of birth, and mother's maiden name can constitute "sensitive personally identifiable information."

The Safe Harbor

A significant safe harbor in the legislation allows covered entities to avoid giving notice if a risk assessment is performed that concludes that, "no significant risk that the security breach has resulted in, or will result in, harm to the individuals whose…"

information was breached. The risk assessment must be disclosed to the United States Secret Service, but the bill does not specify whether the risk assessment or basic statistical data about the breach will be made publicly available.

California law has no safe harbor for risk of harm to individuals. California Civil Code 1798.82(a) specifies that notice is required whenever, "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

While the legislation broadens the types of identifiers subject to security breach notification, the "significant risk" safe harbor creates a loophole that could allow entities to "look the other way" in order to avoid giving notice. This is a significant tradeoff.

Furthermore, it introduces the concept of "harm" into privacy law. Privacy law generally does not require individuals to demonstrate injury in order to recover for an invasion of privacy. Most privacy statutes provide money damages by default if a violation is proven.

Harm is also inappropriate because it is a subjective standard, and it is often equated with physical injury, which is rare in privacy violations. A more appropriate standard would be "misuse" of personal information. "Use" of personal information is well understood in privacy law; many privacy statutes set forth acceptable and unacceptable uses of data.

Misuse is more intuitive, more flexible, and more applicable to a situation where data is stolen but the wrongdoer intends some other type of action than identity theft. Individuals may have particularized sensitivity to having personal information released. For instance, the release of basic contact information of a victim of domestic violence

could cause harm completely unrelated to identity theft or fraud, although the institution experiencing the breach would not perceive this problem, and conclude that there is no significant risk of harm to the individual. Similarly, victims of stalking live with the same risks. Information may be accessed and disclosed simply to embarrass another, or in the case of the Hewlett-Packard pretexting controversy, to investigate another person in an invasive way. All of these risks could be covered by the concept of misuse of information.

We believe that security breach notification laws should favor disclosure over non-disclosure. Allowing the entity that experienced the breach, rather than the individual who may be affected by it, to decide whether to give notice favors non-disclosure. A better standard would be to place the onus on the entity to certify that there is no reasonable risk of misuse of information.

The risks of non-disclosure could be addressed by requiring public, statistical reporting on the breach to a federal agency. Appendix A has two examples of forms required for centralized reporting in New York and North Carolina. These forms contain basic but critical information that individuals can use after a breach occurs, including the date on which the breach occurred, the date when notice was issued, the number of people affected, contact information for the entity, and a simple explanation of what happened. Such reporting could provide a check upon entities that seek to avoid giving notice inappropriately.

The Financial Fraud Prevention Exemption

The financial fraud prevention exemption allows any business entity to be exempt from the notice requirement if it uses or participates in a security program that blocks

unauthorized financial transactions. This exemption is intended to limit the duty to give notice of security breaches where credit card numbers alone are lost or stolen.

This exemption should be considered carefully. It essentially is a sector-specific exemption from a broad information security law. It is not clear why credit card companies, a sector whose products have been identified with the largest data breaches, should be given special, preferential treatment here. Many of the largest information security breaches, ones that led to an understanding that there were weaknesses in compliance with the Payment Card Industry Data Security Standard, would never have come to light if this exemption were in place.

Additionally, in effect, the exemption mandates the use of a specific technological approach to preventing fraud.

Requiring notice in situations where the security program fails and fraud or unauthorized transactions have occurred is insufficiently narrow. Entities often cannot determine basic information about a breach. It is likely that an investigation into a breach could not determine whether that specific breach led to fraud or authorized transactions.

Contents of Notice

The bill specifies that notices sent to individuals include a description of the information stolen, a toll-free number of the entity that experienced the breach, and contact information for the major consumer reporting agencies.

It is important that other information be included as well. We have found that some entities' breach notification letters lack basic information. In some cases, the letters are undated. In others, the timeframe of the breach is not disclosed.

There is also a risk that disclosure may be obscured by promotional text. For instance, in Appendix B, we attach a breach notification letter from H&R Block. Unlike other breach notification letters, the H&R Block one does not advise the reader of the security incident until the second paragraph. The first paragraph only discusses a company promotion and notes how useful its product is.

Notices can be written so as to discourage readership. For instance, in *Ting v. AT&T*, a district court found that AT&T conducted research to develop a notice regarding new contract terms that consumers would be likely ignore.[5] Legislation should anticipate and discourage such efforts.

S. 495, the Personal Data Privacy and Security Act of 2007

Senator Leahy's S. 495, the Personal Data Privacy and Security Act of 2007, incorporates much of the same language of S. 239. In differs in several important ways, and these differences make S. 239 a superior bill. Three provisions of S. 495 are problematic and will limit the policy objectives of security breach notification laws.

First, S. 495 exempts a broader scope of public record information from notification duties than S. 239. S. 495 would create a notice loophole in cases where an entity had a database of sensitive personal information stolen, so long as the data derived from a public record.

---

[5] "Another part of AT&T's research, the Qualitative Study, concluded that after reading the bolded text in the cover letter which states 'please be assured that your AT&T service or billing will not change under the AT&T Consumer Services Agreement; there's nothing you need to do,' 'at this point most would stop reading and discard the letter.' (J. Ex. 9-9.) One of the authors of the study did not find this conclusion to be a cause of concern, and no one on the detariffing team ever expressed concern to her about this conclusion." *Ting v. AT&T*, 182 F. Supp. 2d 902 (N.D. Cal. 2002).

This loophole is problematic, because sensitive information contained within public records often exist in "practical obscurity." That is, they are public records, but they are stored in media generally inaccessible to the public. Once aggregated, these records create a powerful new vector for misuse of personal information.

Just imagine the impact to untold numbers of Americans who have purchased a home, and in the process, had their Social Security numbers filed on the deed. Those Social Security numbers are essentially locked in paper public records across the country. If a company collects that information and digitizes it, thereby making it more accessible to wrongdoers, why should it be exempt from security breach notification?

The Supreme Court has recognized that aggregations of otherwise public information create new risks to privacy. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Court held that disclosure of FBI-aggregated rap sheets, detailing criminal histories, violated the privacy exemption of the Freedom of Information Act. Although the data contained in the compilation of the rap sheets were technically public, they were distributed across the country in documents that were difficult to access. The Court observed that in "an organized society, there are few facts that are not at one time or another divulged to another." It logically flows that an aggregation of these facts could end individuals' right to privacy. The Court appropriately recognized that there is a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole."[6]

---

[6] 489 U.S. at 763 (1989).

In aggregating information from obscure public records, entities make it more likely that this information can be misused. If such an entity suffers a breach, it is just as serious as one where the information was collected by other means. Such an exemption undermines the public policy objectives of security breach notification laws, and may create incentives for entities to inject sensitive personal information into the public record so that privacy laws do not cover it. The broader language from S. 495 should not be included in S. 239.

Second, S.495 provides immunity to the proposed crime of intentionally and willfully concealing a security breach. Individuals qualify for this immunity if they inform the Secret Service of the security breach risk assessment and the agency does not direct the entity to give notice within ten days. We think it extremely unlikely that the Secret Service will have the capacity to routinely review and act upon risk assessments with ten days of their receipt. It will thus make this protection against wrongful concealment illusory and impossible to enforce. This immunity provision should not be included in S. 239.

Finally, S. 239 requires the Secret Service to issue a report to Congress on security breaches. S. 495 limits this important report by prohibiting it from containing any information from a risk assessment. The Secret Service's report should not be limited in this way. For instance, the agency may want to report examples of risk assessments that, in its opinion, were inadequate or demonstrated poor security procedures. This provision should not be included in S. 239.

Identity Theft Reporting

Another aspect in which research could be used to aid policy development on identity theft is to require lending institutions to report basic data about the crime. While there is widespread agreement that identity theft causes financial damage to consumers, creditors, retail establishments, and the economy as a whole,[7] not enough is known about the contours of the crime. We do not have reliable statistics to measure how much of it there is, the relative rates of credit card fraud or "new account" thefts, or how much the crime impacts the economy.

The lack of data on identity theft causes serious problems. As a result, we cannot determine the scope of the crime and the resources that should be allocated to it. We cannot determine whether various consumer protection interventions have been effective. We cannot tell whether consumers, regulators, and businesses are over or under reacting to the crime. We cannot determine whether identity theft is more or less prevalent, or more or less severe than a year ago. We cannot determine how the costs of the crime are being distributed back upon society.

The inability to fully understand the crime stems from the methods used to measure it--what we do know has been learned through telephone and internet surveys. While well-intentioned, and valuable for some purposes in the identity theft policy debate, these surveys cannot completely document the contours of the crime.

More fundamentally, surveys ask the wrong people about the crime. The surveys performed seek to obtain information about the crime from victims, individuals who have

---

[7] GOVERNMENT ACCOUNTABILITY OFFICE, IDENTITY THEFT, AVAILABLE DATA INDICATE GROWTH IN PREVALENCE AND COST GAO-02-424T (Feb. 14, 2002), available at http://www.gao.gov/new.items/d02424t.pdf.

the most limited view of the problem. Victims often cannot tell how the crime occurred, how their information was stolen, or who stole it. Emerging forms of the crime, such as "synthetic identity theft" (also known as fictitious identity theft), occur in such a way that the individual whose data was used never becomes aware of the crime, and thus cannot report being a victim in a survey poll.

A solution can be found in gathering information from the entity that knows the most about the crime—the lending institution. If "lending institutions," companies that actually extend credit (such as banks and credit card companies) and those that control access to accounts (including payment companies such as Paypal and Western Union), were required to provide statistical data about the crime, a more complete and focused picture would emerge. Lending institutions have not provided this information because it could cause embarrassment and because it could attract unwanted regulatory attention.

In a new paper, Chris Hoofnagle proposes that lending institutions should be required to disclose 1) how many identity theft incidences they suffered or avoided, 2) the form of identity theft attempted (i.e. new account fraud, credit card fraud, etc.) and the product targeted (mortgage loan, credit card, etc), and 3) the amount of loss suffered or avoided.[8]

This proposed intervention is relatively simple and does not require extensive regulatory mandates. While there are many challenges, practically and politically, to implementing it, it would result in great benefit to the public. It will enable benchmarking and the identification of additional consumer protections that work and those that do not. It will help regulators and law enforcement allocate the proper

[8] Chris Jay Hoofnagle, *Identity Theft: Making the Known Unknowns Known* (March 2007), available at http://ssrn.com/abstract=969441

resources to fight the crime. It will help clear the air of suspicious polling mischief, the release of surveys that have used questionable assumptions to pin the blame of identity theft to the victims of the crime.

Credit Freeze

Finally, we wish to briefly address the merits of and need for the ability for individuals to have credit freeze rights. Credit freeze gives individuals the option to have more control over their credit reports, while allowing the information to flow for legitimate business purposes, such as to maintain existing accounts.

Credit freeze is necessary because of lax credit granting practices that have made it impossible for consumers to avoid identity theft. This is because the credit reporting system law treats credit issuers, such as retailers and credit card issuers, as trusted insiders. As trusted insiders, credit issuers can easily gain access to reports with or without legal justification.

Furthermore, these trusted credit issuers have not adopted sound measures for determining the actual identity of credit applicants. Such protocols allow identity thieves to open new accounts in others' names. And the harm of identity theft is heightened by the alacrity with which credit grantors issue credit. Competition in the credit markets motivates companies to issue first, and the ask questions later. This allows identity thieves to quickly obtain multiple credit lines.

There is no better illustration of this problem than the rise of "synthetic identity theft" cases. In synthetic identity theft cases, the impostor creates a new identity using some information from a victim that is enhanced with fabricated personal information.[9]

---

[9] FDIC, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT (Dec. 14,
Mulligan & Hoofnagle, IDENTITY THEFT:
INNOVATIVE SOLUTIONS FOR AN EVOLVING PROBLEM

For instance, the impostor may use a real Social Security number, but a falsified name and address. Since this synthetic identity is based on some real information, and sometimes supplemented with artfully created credit histories, it can be used to apply for new credit accounts.

Examples of mistakes in credit granting abound in the media, and bring into question whether consumers can do anything to avoid identity theft, short of freezing their credit report:

- One consumer took an unsolicited credit card offer, ripped it up, reassembled it with tape, and then submitted it to a bank with a change of address. The bank issued the card, and even sent it to the different address, thus demonstrating that a thief could easily use even a torn-up offer for fraud.[10]
- Chase Manhattan bank issued a platinum visa card to "Clifford J. Dawg." In this instance, the owner of the dog had signed up for a free e-mail account in his pet's name and later received a pre-approved offer of credit for "Clifford J. Dawg." The owner found this humorous and responded to the pre-approved offer, listing nine zeros for the dog's Social Security number, the "Pupperoni Factory" as employer, and "Pugsy Malone" as the mother's maiden name. The

---

2004), available at http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html; Fred H. Cate, *Information Security Breaches and the Threat to Consumers* (Sept. 2005), available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/1280/Information_Security_Breaches.pdf.

[10] Bob Sullivan, *Even torn-up credit card applications aren't safe*, MSNBC, Mar. 14, 2006, available at http://redtape.msnbc.com/2006/03/what_if_a_despe.html.

owner also wrote on the approval: "You are sending an application to a dog! Ha ha ha." The card arrived three weeks later.[11]

- Credit has been offered and issued to other dogs, including Monty, a Shih-Tzu who was extended a $24,600 credit line.[12] It also has been granted to children and babies.[13]
- In *Vazquez-Garcia v. Trans Union de Puerto Rico*, Sears issued a credit card to an impostor who used the victim's Social Security number but wrong address and date of birth. The victim was a resident of Puerto Rico, but several cards were issued to an impostor using a Nevada address.[14]

---

[11] *Dog Gets Carded*, Wash. Times (Jan. 30, 2004), available at http://washingtontimes.com/upi-breaking/20040129-031535-6234r.htm; *Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBC San Diego (Jan. 28, 2004), available at http://www.nbcsandiego.com/money/2800173/detail.html.

[12] *Identity thieves feed on credit firms' lax practices*, USA TODAY, Sept. 12, 2003, p. 11A; Kevin Hoffman, *Lerner's Legacy: MBNA's customers wouldn't write such flattering obituaries*, CLEVELAND SCENE, Dec. 18, 2002; Scott Barancik, *A Week in Bankruptcy Court*, ST. PETERSBURG TIMES, Mar. 18, 2002, p 8E.

[13] IDENTITY THEFT RESOURCE CENTER, FACT SHEET 120: IDENTITY THEFT AND CHILDREN, available at http://www.idtheftcenter.org/vg120.shtml.

[14] 222 F. Supp. 2d 150 (D.P.R. 2002). Many other cases demonstrate that credit can be obtained by imposters, even when they use incorrect personal information. In *Nelski v. Pelland*, 2004 U.S. App. LEXIS 663 (6th Cir. 2004), Ameritech opened an account for an impostor who used the victim's name, but a different address and slightly different Social Security number. In *Dimezza v. First USA Bank, Inc.*, 103 F. Supp. 2d 1296 (D.N.M. 2000), First USA Bank issued a credit card to an impostor who used the victim's Social Security number but a different first name and address. In *Alward v. Fleet Bank*, 22 F.3d 616 (8th Cir. 1997), Fleet Bank issued two credit cards in the name of the victim to a New York address. The victim had never lived in that state. In *Fritzhand v. Discover Financial Services*, 800 N.Y.S.2d 316 (New York Supreme Court, Nassau County 2005), Discover accepted a $14,000 balance transfer from a fraudulently-obtained American Express account. Both accounts were opened with the victim's name but with a fictitious address. In *Farley v. Williams & U.C. Lending*, 2005 U.S. Dist. LEXIS 38924 (W.D.N.Y. 2005), a store line of credit and a Citibank platinum card were issued to an impostor using the victim's name and Social Security number but the impostor's home address.

These anecdotal examples from news reports and litigation demonstrate that in some cases, credit is issued to people who obviously are impostors. Simple tools long available to lending institutions, such as address verification databases, could have prevented the frauds. But the individual has no ability to ensure that lending institutions are using these tools, nor can they avoid these unsophisticated cases of identity theft.

Credit freeze could put consumers back in control of their credit reports, and thus, act as a shield against even the most irresponsible granting practices.

Conclusion

Madame Chairwoman, thank you again for inviting us to participate in this hearing. As our research into security breach notification and investments in privacy and security progresses we will update the Committee about our findings. We would be honored to speak with the Committee in depth about the issues raised above and other proposals to reduce the risks of identity theft and improve information and network security more broadly.

Reporting Form
For Business, Individual or NY State Entity reporting a "Breach of the Security of the System"
Pursuant to the Information Security Breach and Notification Act (General Business Law §889-aa; State Technology Law §208)

Name of Business, Individual or State Entity: H&R Block
Date of Discovery of Breach: December 19, 2005
Estimated Number of Affected Individuals: 28,750
Date of Notification to Affected Individuals: December 22, 2005
Manner of Notification: [X] written notice
[ ] electronic notice (email)
[ ] telephone notice

Are you requesting substitute notice? [ ] Yes [X] No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

As part of a promotional campaign, H&R Block recently mailed free copies of our TaxCut® tax preparation software to a select group of individuals. For a small percentage of recipients of this mailing, we inadvertently included some personal information in the mailing label. Embedded within the more than 40-character source code were the nine digits of the recipient's Social Security Number (SSN). These digits were not formatted in a way that identified them as an SSN, and to an unknowing observer they would appear to be random digits within a very long character string. However, the recipient may have recognized his or her own SSN. H&R Block quickly recognized the error and is voluntarily notifying all affected recipients to advise them of the situation and offer helpful information. The actual notice provided to affected New York residents is included as Attachment A.

Name of Business or Individual Contact Person: Murray Walton
Title: Vice President and Chief Compliance Officer
Telephone number: 816-932-8414
Email: mwalton@hrblock.com
Dated: December 29, 2005
Submitted by: Murray Walton
Title: Vice President and Chief Compliance Officer
Address: 4400 Main Street
Kansas City, MO 64111
Email: mwalton@hrblock.com
Telephone: 816-932-8414 Fax: 816-932-8462

North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the Breach: _____
Address: _____
_____
Telephone: _____
Fax: _____
Email: _____

PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: _____

Date the Security Breach was discovered: _____

Estimated number of affected individuals: _____

Estimated number of NC residents affected: _____

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b): _____
_____

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: _____
_____

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. _____ If so, please describe the security measures protecting the information: _____
_____

Describe any measures taken to prevent a similar Security Breach from occurring in the future: _____
_____

Date affected NC residents were/will be notified: _____

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c)): _____
_____

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified?
(pursuant to N.C.G.S. § 75-65(e))
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

- ☐ written notice
- ☐ electronic notice (email)
- ☐ telephone notice
- ☐ substitute notice

Signature: _____ Date: _____
Contact Person, Title: _____
Address: _____
(if different from above) _____
Telephone: _____ Fax: _____ Email: _____

Attachment A
Notice to New York Residents

December 22, 2005

[FirstName] [LastName]
[Address]
[City], [State] [ZIP]

Dear [FirstName] [LastName]:

Recently we mailed you a free copy of our TaxCut® software. We believe that this complimentary software will meet your 2006 tax preparation needs, based on our prior experience with you as an H&R Block client. We hope that you will try TaxCut and find it to be a great solution for filing your next tax return.

However, since we originally sent you this CD, we have become aware of a mail production situation that has affected a small percentage of recipients, including you. Due to human error in developing the mailing list, the digits of your social security number (SSN) were used as part of your mailing label's source code, a string of more than 40 numbers and characters. Fortunately, these digits were embedded in the middle of the string, and they were not formatted in any manner that would identify them as an SSN.

Nevertheless, we sincerely apologize for this inadvertent error, which is completely inconsistent with our strict policies to protect our clients' privacy. Our internal policies limit the use of client SSNs for purposes other than tax preparation. Furthermore, our internal procedures require that mailing source codes are formulated in a manner that excludes use of any sensitive or confidential information. Please know that we have conducted a thorough internal review of this matter, and are taking actions to ensure this does not re-occur.

Again, please understand that the digits of your SSN were embedded in the middle of a lengthy source code, and they were not formatted in a manner that identifies them as an SSN. As a result, we believe the exposure of your SSN digits was limited to you alone, since you are the only person who would recognize their significance. Nonetheless, we suggest that you destroy the wrapper and mailing label of the free TaxCut CD we sent you. If you would like more information about this incident, please visit www.taxcut.com/answers, a special Website that contains additional details and an e-mail link for contacting us with your questions.

On behalf of the more than 100,000 associates of H&R Block, allow me to apologize for this unfortunate situation. Through 50 tax seasons, H&R Block has earned a reputation as a valued, trustworthy ally to our clients, and we sincerely hope that you will find the free TaxCut CD and our information-packed taxcut.com Website to be helpful tools for the 2006 tax filing season.

Sincerely,

Tom Allanson

Tom Allanson
Senior Vice President & General Manager
H&R Block Digital Tax Solutions

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY

of the

SENATE COMMITTEE ON THE JUDICIARY

on

Identity Theft: Innovative Solutions for an Evolving Problem

Washington, DC

March 21, 2007

I. INTRODUCTION

Madam Chairman, Senator Kyl, and members of the Subcommittee, I am Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the important and interrelated issues of identity theft; data security; and the collection, use, and disclosure of Social Security numbers ("SSNs").

Identity theft is a pernicious crime and controlling it is a critical component of the Commission's consumer protection mission. This testimony describes the nature and scope of the identity theft problem and the critical role that SSNs play both in creating and solving the problem. This testimony also will summarize the Commission's efforts to combat identity theft through its law enforcement actions against companies that failed to reasonably protect consumer data, its participation on the Identity Theft Task Force, and its extensive consumer and business education and outreach efforts.

II. THE IDENTITY THEFT PROBLEM

Identity theft has become a serious concern in our information-based economy. Millions of consumers are victimized by this crime every year.[2] Generally speaking, there are two varieties of identity theft: the takeover or misuse of existing credit card, debit card, or other accounts ("existing account fraud"); and the use of stolen information to open new accounts in

---

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

[2] *See, e.g.*, http://www.javelinstrategy.com/uploads/701.R_2007IdentityFraudSurveyReport_Brochure.pdf.

the consumer's name ("new account fraud"). New account fraud, although less prevalent, typically causes considerably more harm to consumers in out-of-pocket expenses and time necessary to repair the damage.[3]

Beyond its direct costs, concerns about identity theft harm our economy by threatening consumers' confidence in the marketplace generally, and in electronic commerce specifically. A recent Wall Street Journal/Harris Interactive survey, for example, found that, as a result of fears about protecting their identities, 30 percent of consumers polled were limiting their online purchases, and 24 percent were cutting back on their online banking.[4]

Identity theft has many causes, but this testimony will focus on two of them: the failure to protect consumers' sensitive personal information, which can lead to data breaches; and the availability of SSNs, with which identity thieves can open new accounts in consumers' names. The government and private sector must continue to work together to reduce the opportunities for thieves to obtain consumers' personal information, and make it more difficult for thieves to misuse the information if they do obtain it.

---

[3] Federal law limits consumers' liability for unauthorized credit card charges to $50 per card as long as the credit card company is notified within 60 days of the unauthorized charge. *See* 12 C.F.R. § 226.12(b). Many credit card companies do not require consumers to pay the $50 and will not hold consumers liable for the unauthorized charges, no matter how much time has elapsed since the discovery of the loss or theft of the card.

[4] *See* Jennifer Cummings, *Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft*, The Wall Street Journal Online, May 18, 2006, http://www.harrisinteractive.com/news/newsletters/WSJfinance/HI_WSJ_PersFinPoll_2006_vol2_iss05.pdf.

III. COMMISSION ACTIVITIES TO COMBAT IDENTITY THEFT

A. Law Enforcement on Data Security

One important way to keep sensitive information out of the hands of identity thieves is by ensuring that those who maintain such information adequately protect it. The Commission plays an active role in furthering this goal through law enforcement action against businesses that fail to implement reasonable security measures to protect sensitive consumer data.

Public awareness of, and concerns about, data security have reached new heights as reports about the latest data breaches of sensitive personal information continue to proliferate. Recent breaches have touched both the public and private sectors. Of course, not all data breaches lead to identity theft; in fact, many prove harmless or are caught and addressed before any harm occurs. Nonetheless, some breaches - especially those that result from deliberate actions, such as hacking, by criminals - have led to identity theft.

A number of bills have been introduced in the past two sessions of Congress that would require businesses that maintain sensitive consumer information to have reasonable protections in place to prevent unauthorized access, as well as to require companies that suffer a data breach to provide notice to affected consumers. Pending the enactment of broad data security legislation, the FTC enforces several laws that contain data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, contains data security requirements for financial institutions.[5] The Fair Credit Reporting Act

---

[5] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

("FCRA") includes certain due diligence requirements for consumer reporting agencies[6] and safe disposal obligations for companies that maintain consumer report information.[7] In addition, the FTC has enforced the Federal Trade Commission Act's proscription against unfair or deceptive acts or practices in cases where a business made false or misleading claims about its security procedures, or where its failure to employ reasonable security procedures caused substantial consumer injury.[8]

Since 2001, the Commission has brought fourteen cases challenging businesses that failed to reasonably protect sensitive consumer information that they maintained.[9] In a number of these cases, the Commission alleged that the company had misrepresented the nature or extent of its security procedures in violation of the FTC Act's prohibition on deceptive practices.[10] In addition, in several of the cases, the alleged security inadequacies led to breaches that caused

---

[6] 15 U.S.C. § 1681 et seq. The FCRA specifies that consumer reporting agencies may provide consumer reports only for enumerated "permissible purposes," and requires that they have reasonable procedures to verify the identity and permissible purposes of prospective recipients of their reports.

[7] The FTC's implementing disposal rule is at 16 C.F.R. Part 382.

[8] 15 U.S.C. § 45(a).

[9] *See generally* http://www.ftc.gov/privacy/index.html.

[10] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Guidance Software, Inc.*, FTC Matter No. 0623057 (Nov. 16, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (March 4, 2005); *In the Matter of MTS Inc., d/b/a/ Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

substantial consumer injury and were challenged as unfair practices under the FTC Act.[11] Some of the cases involved enforcement of the Commission's GLB Act Safeguards Rule or the FCRA.[12]

Probably the best-known FTC data security case was its action against ChoicePoint, Inc. ChoicePoint, a data broker, inadvertently sold sensitive information (including credit reports in some instances) on more than 160,000 consumers to data thieves, who used that information in some cases to commit identity theft. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of its information. For example, the company allegedly approved as purchasers individuals who lied about their credentials, used commercial mail drops and business addresses, and faxed multiple applications from nearby commercial photocopying facilities. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties for violations of the FCRA and $5 million in consumer redress for identity theft victims, and agreed to undertake substantial new data security measures.[13]

---

[11] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (March 7, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

[12] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Nationwide Mortgage Group Inc.*, FTC Docket No. 9319 (April 15, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005). In the *Nations Title, Nationwide Mortgage Group,* and *Sunbelt Lending Services* cases, the Commission also alleged that the companies violated the GLB Act's privacy provisions and the FTC's implementing Privacy Rule, which, among other things, require financial institutions to provide notices to their customers describing their information-sharing policies.

[13] *See* FTC Press Release, *ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.html. The Commission has mailed more than

The Commission's most recent data security enforcement action involved Guidance Software, Inc., a marketer of software and related services for investigating and responding to computer breaches and other security incidents. According to the FTC complaint, Guidance, in contrast to its claims, failed to implement simple, inexpensive and readily available security measures to protect consumers' data, for example, by permanently storing credit card information in clear, readable text rather than encrypting or otherwise protecting it.[14]

Although the Commission's data security cases have been brought under different laws, they share common elements: the vulnerabilities were multiple and systemic, and readily-available and often inexpensive measures were available to prevent them. Together, the cases stand for the proposition that companies should maintain reasonable and appropriate measures to protect sensitive consumer information.

The FTC Safeguards Rule promulgated under the GLB Act serves as a good model of this approach. Firms covered by the Rule must prepare a written plan; designate an official with responsibility for the plan; identify, assess, and address foreseeable risks; oversee their service providers handling of information; monitor and evaluate the program for effectiveness; and adjust the plan as appropriate. The Rule specifies that what is "reasonable" will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue. This standard recognizes that there cannot be "perfect" security, and that data breaches can occur despite the maintenance of reasonable precautions to prevent them.

1,400 claims forms to possible victims and has created a website where consumers can download claims forms and obtain information about the claims process.

[14] *In the Matter of Guidance Software, Inc.*, FTC Matter No. 0623057 (Nov. 16, 2006).

It also is a flexible and adaptable standard that accounts for the fact that risks, technologies, and business models change over time, and that a static technology-based standard would quickly become obsolete and might stifle innovation in security practices. The Commission will continue to apply the "reasonable procedures" principles in enforcing existing data security laws.

B. Participation in the Identity Theft Task Force

On May 10, 2006, the President established an Identity Theft Task Force. Comprised of 18 federal agencies, the Task Force is chaired by Attorney General Alberto Gonzales and co-chaired by FTC Chairman Deborah Platt Majoras. The mission of the Task Force is to develop a comprehensive national strategy to combat identity theft.[15] The President specifically directed the Task Force to make recommendations on ways to improve further the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution.

On September 19, 2006, the Task Force published a set of interim recommendations on measures that could be implemented immediately to help address the problem of identity theft.[16] Broadly, these recommendations are organized around the principles of prevention (improving government handling of sensitive data and improving authentication methods), victim assistance, and law enforcement. These recommendations have been implemented or are in the process of being implemented.

---

[15] Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

[16] *See* FTC Press Release, *Identity Theft Task Force Announces Interim Recommendations* (Sept. 19, 2006), *available at* www.ftc.gov/opa/2006/09/idtheft.htm.

To supplement its research and analysis, on December 26, 2006, the Task Force solicited public comment on a list of possible additional recommendations.[17] The Task Force received approximately 150 comments, representing the views of trade associations, consumer advocacy groups, and identity theft victims. Many comments concerned the use of SSNs, their value in matching consumers to their information, and possible alternative identifiers. In addition, the Task Force received many comments stressing the need to enhance the prosecution of identity theft and to promulgate national standards for data security. The Task Force is in the process of reviewing the comments and preparing a final strategic plan and recommendations.

C. Consumer and Business Education

The Commission has undertaken substantial efforts to increase consumer and business awareness of the importance of protecting data and taking other steps to prevent identity theft. The Commission works to empower consumers by providing them with the knowledge and tools to protect themselves from identity theft and to deal with the consequences when it does occur. The Commission receives about 15,000 to 20,000 contacts each week on how to recover from identity theft, or how to avoid becoming a victim in the first place. Callers to our hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft. The FTC's identity theft primer[18] and victim recovery guide[19] are widely available in print

---

[17] *See* FTC Press Release, *Identity Theft Task Force Seeks Public Comment* (Dec. 26, 2006), *available at* http://www.ftc.gov/opa/2006/12/fyi0688.htm.

[18] *Avoid ID Theft: Deter, Detect, Defend, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm.

[19] *Take Charge: Fighting Back Against Identity Theft, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm.

and online. The Commission has distributed over 2 million copies of the primer and has recorded over 2.4 million visits to the Web version.

Last year, the Commission launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend." It includes direct-to-consumer brochures, as well as training kits and ready-made materials (including presentation slides and a video) for use by businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. The Commission has distributed over 1.5 million brochures and 40,000 kits to date. The Commission also has partnered with other organizations to broaden its reach. As just one example, the U.S. Postal Inspection Service recently initiated an outreach campaign to place FTC educational materials on subway cars in New York, Chicago, San Francisco, and Washington D.C.

The Commission also sponsors a multimedia website, OnGuard Online,[20] designed to educate consumers about basic computer security, including the importance of not disclosing personal information such as SSNs to possible fraudsters. OnGuard Online was developed in partnership with other government agencies and the technology sector, and since its launch has attracted more than 3.5 million visits.

The Commission directs its outreach to businesses as well. Just this month, the FTC released a new business education guide related to security.[21] Most companies have some information in their files - names, Social Security numbers, credit card numbers - that identifies

---

[20] *See* http://www.onguardonline.gov/index.html.

[21] *Protecting Personal Information: A Guide for Business, available at* http://www.ftc.gov/infosecurity.htm. Other business publications on data security and responding to data breaches are available at http://www.ftc.gov/bcp/edu/microsites/idtheft.htm.

their customers and employees. The Commission has heard from some businesses, particularly smaller businesses, that they were not sure what data security measures they should take to protect such sensitive information from falling into the wrong hands. FTC staff therefore developed a brochure that articulates the key steps that are part of a sound data security plan. The Commission anticipates that the brochure will prove to be a useful tool in alerting businesses to the importance of data security issues and give them a solid foundation on how to address those issues.

IV. PROTECTING AGAINST MISUSE OF SOCIAL SECURITY NUMBERS

Data breaches involving SSNs can be particularly harmful to consumers, because the SSN in many cases is the key piece of information that can enable criminals to perpetrate new account fraud. Making SSNs more difficult to obtain by criminals - and more difficult to use - is critical in the fight against this kind of identity theft.

A. The Uses and Sources of SSNs

SSNs play a vital role in our economy, enabling businesses, government, and others to match information to the proper individual. For example, consumer reporting agencies use SSNs to ensure that the data furnished to them is placed in the correct file, and that they are providing the right credit report for the right consumer. SSNs also are used in locator databases to find lost beneficiaries, witnesses, and law violators and to collect child support and other judgments. Employers must collect SSNs for tax reporting purposes, and health care providers may need them to facilitate Medicare reimbursement.

SSNs are available from both public and private sources. Public records in city and county offices across the country, including birth and death records and voter registrations, often

contain individuals' SSNs. There also are a number of private sources of SSNs, including consumer reporting agencies that include the SSN as part of the "credit header" information on consumer reports. Information brokers also collect personal information, including SSNs, from a variety of sources and compile and resell that data to third parties.

B. Current Laws Restricting the Use or Disclosure of SSNs

There are several federal and state laws and regulations that restrict the use or disclosure of SSNs in certain contexts.[22] Of most relevance is the GLB Act and its implementing regulations ("Privacy Rule"), which prohibit financial institutions from disclosing nonpublic personal information, including SSNs, to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of the disclosure.[23] The GLB Act and Privacy Rule include a number of exceptions under which disclosure is permitted without having to provide notice and opt out, including for purposes of credit reporting, fraud prevention, law enforcement, and compliance with judicial process.[24] Entities that receive nonpublic personal information under one of these exceptions are subject to the reuse and redisclosure restrictions of the Privacy Rule, even if those entities are not themselves financial institutions. More specifically, recipients may use or disclose the information only "in the ordinary course of

---

[22] For example, the FCRA, as amended by the Fair and Accurate Credit Transactions Act of 2003, requires consumer reporting agencies, upon the consumer's request, to truncate the SSN on reports provided to consumers. 15 U.S.C. § 1681g(a)(1)(A). The Driver's Privacy Protection Act prohibits state motor vehicle departments from disclosing personal information, including SSNs, in motor vehicle records, subject to several exceptions. 18 U.S.C. §§ 2721-25.

[23] 16 C.F.R. Part 313, implementing 15 U.S.C. § 6801 *et seq.*

[24] 15 U.S.C. § 6802(e).

business to carry out the activity covered by the exception under which ... the information [was received]."[25]

C. Limiting the Use and Disclosure of SSNs

As described above, the SSN is valuable in enabling entities to match information to consumers. With 300 million Americans, many of whom share the same name, the SSN presents significant advantages as a means of identification because of its uniqueness and permanence. The misuse of SSNs, however, can facilitate identity theft. The challenge is to find the proper balance between the necessity of keeping SSNs out of the hands of identity thieves, while giving businesses and government sufficient means to match information to the correct person. Excessive restrictions on the use of SSNs could have a deleterious impact on such important purposes as public health, criminal law enforcement, and anti-fraud and anti-terrorism efforts.

SSNs are available to identity thieves, in part, because they are widely used as consumer identifiers, i.e., to associate information with particular individuals. For example, SSNs sometimes are used as identification numbers displayed on identification cards. These SSNs are extremely valuable to identity thieves. They frequently are used by creditors and other benefit providers to access information (such as a credit report) that is necessary to open an account or provide other benefits. Unless the creditor obtains sufficient additional authenticating information - i.e., information proving that the individual is who he purports to be - a thief with a consumer's name and SSN, and perhaps additional information or documentation, may be able to open an account by impersonating the consumer. In short, the SSN is both widely available and valuable to identity thieves.

---

[25] 16 C.F.R. Part 313.11(a).

Preventing the misuse of SSNs, therefore, can follow two paths. First, the unnecessary use and disclosure of SSN as an identifier can be reduced. The Identity Theft Task Force is working toward this goal. For example, one of its interim recommendations was that the federal government review its collection and use of SSNs with the goal of eliminating them wherever possible.

Second, to prevent misuse of SSNs, improved methods of authenticating consumers can be promoted so that, even if the SSN falls into the hands of an identity thief, that SSN is less valuable. On April 23 and 24, 2007, the Commission will sponsor a workshop on authentication. The workshop is designed to facilitate discussions among knowledgeable parties about the technological and policy issues surrounding the development of improved authentication procedures.[26]

V. CONCLUSION

Identity theft remains a serious problem in our economy, causing enormous harm to consumers and businesses and threatening consumer confidence in the marketplace. To succeed in the battle against identity theft, government and the private sector, working together, must make it more difficult for thieves to obtain the information they need to steal identities, and make it more difficult to use that information if they obtain it. There are several actions that should be taken to further these goals. To prevent thieves from obtaining sensitive information, government and the business community must better protect their data, and must consider what information they collect and maintain from or about consumers and whether they need to do so.

---

[26] *See Proof Positive: New Directions for ID Authentication*, 72 Fed. Reg. 8381 (Feb. 26, 2007); http://www.ftc.gov/bcp/workshops/proofpositive/index.html.

In this regard, eliminating unnecessary collection, use, and disclosure of Social Security numbers - an important tool of identity thieves - can play a key role. To keep thieves from using the information they do procure to steal identities, better means of consumer authentication must be developed and implemented. The Commission will continue and strengthen its law enforcement efforts, as well as its education and outreach to guide and empower businesses and consumers to fight back against identity theft.

Department of Justice

STATEMENT

OF

RONALD J. TENPAS
ASSOCIATE DEPUTY ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE

ON

IDENTITY THEFT

BEFORE

THE SUBCOMMITTEE ON TERRORISM, TECHNOLOGY
AND HOMELAND SECURITY
THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

MARCH 21, 2007

Good morning, Madam Chairman and Members of the Subcommittee. I am pleased to appear before you today, on behalf of the Department of Justice, to testify on the topic of identity theft. The Department is strongly committed to the aggressive pursuit of identity theft in all forms, because its effects are both pervasive and substantial. A Bureau of Justice Statistics survey found that in just six months in 2004, 3.6 million U.S. households learned that they were victims of identity theft.[1] More recently, a 2007 private-sector survey found that 8.9 million U.S. adults had become victims of identity fraud in the preceding year, leading to losses of nearly $50 billion.[2]

This morning, I would like to speak with you about the dual roles that the Department of Justice is playing in combating identity theft: first, as the prosecuting agency that seeks to bring identity thieves to justice; and second, as one of the two agencies leading the President's Identity Theft Task Force. In doing so, I will focus on the Department's substantial accomplishments in prosecuting identity theft, and on the work of the President's Identity Theft Task Force, which I serve as Executive Director. Since May 2006, the Task Force has been developing a comprehensive strategic plan for the federal government to combat identity theft more effectively. Because the Task Force is in the final stages of preparing its plan for presentation to the President, I cannot speak to the specific, final recommendations that will be contained in the plan. The Task Force, however, released several interim recommendations in September 2006, and I would be pleased to report on those and the status of their implementation.

Identity Theft Prosecutions

The Department works closely with many investigative agencies, including the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), the United States Postal Inspection Service (USPIS), and the Social Security Administration Office of the Inspector General (SSA OIG), to prosecute identity thieves. Federal prosecutors use a wide variety of federal statutes in prosecuting cases that involve identity theft. These include not only the original identity theft statute (18 U.S.C. § 1028(a)(7)) and the aggravated identity theft statute (18 U.S.C. § 1028A(a)), but other federal criminal statutes applicable to fraud, such as wire fraud (18 U.S.C. § 1343), mail fraud (18 U.S.C. § 1341), access device fraud (18 U.S.C. § 1029), financial institution fraud (18 U.S.C. § 1344), and Social Security fraud (42 U.S.C. § 408(a)(7)).

The aggravated identity theft statute enacted in 2004, which carries a mandatory two-year prison sentence, has been a particularly useful tool to the Department in prosecuting identity thieves and ensuring that they receive adequate punishment. Since 2004, DOJ has made increasing use of the aggravated identity theft statute: in Fiscal Year 2006, DOJ charged 507 defendants with aggravated identity theft, up from 226 in Fiscal Year 2005. In many of these cases, the courts have imposed substantial sentences.

---

[1] *See* Bureau of Justice Statistics, U.S. Dep't of Justice, Bulletin: Identity Theft, 2004 (April 2006), *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

[2] *See* JAVELIN STRATEGY & RESEARCH, 2007 IDENTITY FRAUD SURVEY REPORT: IDENTITY FRAUD IS DROPPING, CONTINUED VIGILANCE NECESSARY (February 2007).

Because identity theft can be involved in a wide range of criminal activities, ranging from fraud to organized crime to terrorism, the Department does not limit its prosecutions to any single type of identity theft. Nonetheless, there are several recurring types of criminal activity in the identity theft prosecutions recently brought by the Department.

First, many of the identity theft cases we prosecute involve extensive and often elaborate criminal organizations. The following are just a few examples of these types of identity theft prosecutions:

- On January 24, 2007, in the Southern District of New York, a defendant was sentenced to 34 months imprisonment for his role in a large identity-theft ring that was engaged in, among other things, stealing individual victims' personal identity information, sharing that information over the Internet with other members of the identity-theft ring, and using the information to commit various forms of fraud. The defendant and his co-conspirators stole the identities of at least 175 individuals and victimized a large number of financial institutions. The investigation revealed a large number of e-mails between ring members in which they exchanged credit card numbers, together with expiration dates and three-digit codes. The e-mails also included the personal identity information of a large number of individual victims, including victims' names, addresses, telephone numbers, Social Security numbers, and mothers' maiden names. The defendant and his co-conspirators then used the stolen credit card numbers and identity information to commit various forms of fraud, including using the credit card numbers to make purchases over the Internet.[3]

- On November 21, 2006, in the Eastern District of Virginia, a defendant was sentenced to 134 months imprisonment for aggravated identity theft, production and use of counterfeit credit cards, and conspiracy to utter counterfeit checks. Beginning in August 2005, the defendant and his co-conspirators deposited large-denomination counterfeit checks totaling $318,378.34 into the bank accounts of several local co-conspirators. The defendant and his accomplices obtained over $89,000 from TowneBank before their scheme was detected. During this same period, the defendant enlisted a front desk clerk at a hotel in Virginia Beach to provide him with the credit card information of hotel guests in exchange for cash. Thereafter, the clerk sold to the defendant and another co-conspirator in New York City, the names and credit card information of over 100 hotel guests. These stolen credit card account numbers were then used to produce counterfeit credit cards in the names of co-conspirators. The co-conspirators then used these cards to purchase airplane tickets, hotel rooms and rental cars so that they could travel around the country purchasing high-end electronic items, such as flat screen televisions, which were

[3] *See* U.S. Attorney's Office, Southern District of New York, Press Release (January 24, 2007), *available at* http://newyork.fbi.gov/dojpressrel/pressrel07/identitytheft012407.htm.

then sold for cash. The losses related to the counterfeit card scheme were more than $340,000.[4]

A second category of identity theft cases involves use of the Internet to acquire and trade in people's identifying information on an international scale and other significant instances of unauthorized computer access. The following are just a few examples of the Department's prosecutions of these types of identity thieves:

- On February 9, 2007, in the Eastern District of Virginia, a defendant was sentenced to 94 months for aggravated identity theft, access device fraud, and conspiracy to commit bank fraud. The defendant, who went by the Internet nickname "John Dillinger," was involved in extensive illegal online "carding" activities. He received e-mails or instant messages containing hundreds of stolen credit card numbers, usually obtained through phishing schemes or network intrusions, from "vendors" who were located in Russia and Romania. In his role as a "cashier" of these stolen credit card numbers, the defendant would then electronically encode these numbers to plastic bank cards, make ATM withdrawals, and return a portion to the vendors. Computers seized from the defendant revealed over 4,300 compromised account numbers and full identity information (*i.e.*, name, address, date of birth, social security number, mother's maiden name, etc.) for over 1,600 individual victims.

- In November 2006, in the Western District of Washington, two defendants pleaded guilty to conspiracy to commit identity theft. According to the indictment, one defendant was employed at a janitorial company and worked at night in a U.S. Bank branch. He joined with other conspirators to steal information on more than 200 bank customers. Using that information, the defendants opened credit accounts in the customers names and used those accounts to purchase expensive items such as laptop computers, flat screen televisions, and airline tickets. In addition, they signed up for on-line banking for accounts that had not previously had on-line banking and then used those accounts to pay their own bills and transfer funds to other checking accounts that they then drained. The indictment charged the defendants with more than $200,000 in fraud against dozens of victims.

- On June 28 and 29, 2006, in the District of New Jersey, four defendants were sentenced to prison terms of up to 32 months for conspiracy to commit credit card and bank card fraud, as well as identification document fraud. As part of their earlier guilty pleas, these defendants admitted to their involvement in the Shadowcrew international criminal organization. Using the website www.shadowcrew.com, the Shadowcrew organization had thousands of members engaged in the online trafficking of stolen identity information

---

[4] *See* U.S. Attorney's Office, Eastern District of Virginia, Press Release (November 22, 2006), *available at* http://www.usdoj.gov/usao/vae/Pressreleases/11-NovemberPDFArchive/06/20061122ross_charlesnr.pdf.

and documents, such as drivers' licenses, passports, and Social Security cards, as well as stolen credit card, debit card, and bank account numbers. The Shadowcrew members trafficked in at least 1.7 million stolen credit card numbers and caused total losses in excess of $4 million dollars. The website was successfully shut down following a year-long undercover investigation that resulted in the arrests of 21 individuals in the United States on criminal charges in October 2004. Additionally, law enforcement officers in six foreign countries arrested or searched eight individuals.

A third category of identity theft cases prosecuted by the Department involves health care fraud and theft of patient information. The following are some examples of the Department's prosecutions in this area:

- On January 24, 2007, in the Southern District of Florida, a federal jury convicted a defendant of all eight counts of a superseding indictment, which charged him with conspiring to defraud the United States, computer fraud, wrongful disclosure of individually identifiable health information, and aggravated identity theft. The case involved the theft and transfer of Medicare patient information from the Cleveland Clinic in Weston, Florida. The defendant purchased the patient information from his co-defendant, a former Cleveland Clinic employee, who pleaded guilty on January 12, 2007 and testified against the defendant at trial. The theft resulted in the submission of more than $7 million in fraudulent Medicare claims, with approximately $2.5 million paid to providers and suppliers. This is the first Health Insurance Portability and Accountability Act ("HIPAA") violation case that has gone to trial in the United States. The defendant is scheduled to be sentenced on April 27, 2007.[5]

- On July 7, 2006, in the Southern District of Florida, three defendants who were indicted by a federal grand jury in a multi-million dollar health care fraud were arrested. The indictment charged all three defendants with conspiracy to defraud a health care benefits program (Medicare) and defrauding a health care benefits program (Medicare). It also charged two of the defendants with identity theft for fraudulently utilizing Unique Physician Identification Numbers (UPIN) without the physicians' approval or knowledge. It also charged the third defendant with paying kickbacks and bribes to induce the referral of Medicare beneficiaries.[6]

In addition to our prosecutions, the Department is proud of the investigative efforts and initiatives undertaken by the FBI to combat identity theft. These include the IC3 project, which is a public-private alliance between the IC3 Unit of the FBI and the National White Collar Crime Center. Among other things, IC3 disseminates information on cybercrime and actionable cyber-

---

[5] *See* U.S. Attorney's Office, Southern District of Florida, Press Release (January 24, 2007), *available at* http://miami.fbi.gov/dojpressrel/pressrel07/mm20070124b.htm.

[6] *See* U.S. Attorney's Office, Southern District of Florida, Press Release (July 7, 2006), *available at* http://miami.fbi.gov/dojpressrel/pressrel06/mm20060707.htm.

related investigative leads, including those involving identity theft, to state and local law enforcement. IC3 has also formed an extensive network of relationships with industry, which has been a key to identifying cybercrime and typically associated identity theft.

Many other investigative agencies, too, including the Secret Service and U.S. Postal Inspection Service, have formed crucial partnerships with the private sector in an effort to combat identity theft. The Secret Service, for example, hosts a portal called the e-Information system for members of the law enforcement and banking communities, which provides a forum for members to post the latest information on scams, counterfeit checks, frauds and swindles, and updated Bank Identification Numbers (BINs). In 2005, the USPIS created the Intelligence Sharing Initiative (ISI), a website that allows the Inspection Service and fraud investigators representing retail and financial institutions, as well as major mailers, to openly share information pertaining to mail theft, identity theft, financial crimes, investigations, and prevention methods.

Efforts have also been taken to investigate and arrest identity thieves who operate in foreign countries. For example, between April and November 2006, the FBI's Cyber Division supported "Cardkeeper," a major initiative with the FBI's Richmond, Virginia field office. As part of that initiative, the FBI sent six agents to Bucharest, Romania, to work with the Romanian National Police (RNP) to investigate the Internet intrusions committed by criminals in Romania, and which resulted in harm to U.S. victims. This unprecedented initiative resulted in thirteen arrests in the United States and three searches in Romania. The success of this investigation gave rise to the Romanian Task Force initiative, through which FBI agents are deployed to Romania to work full-time, hand-in-hand with the RNP on cases of mutual interest.

The Department intends to continue to work hand-in-hand with all of our law enforcement partners to aggressively investigate and prosecute identity thieves.

President's Identity Theft Task Force

Background

I would like to turn now to the work of the President's Identity Theft Task Force. On May 10, 2006, President Bush issued an Executive Order that established the Task Force.[7] The Task Force, under the leadership of the Attorney General as Chairman and Federal Trade Commission Chairman Deborah Platt Majoras as Co-Chairman, includes representatives from 17 departments and agencies, including the Departments of Commerce, Health and Human Services, Homeland Security, Treasury, and Veterans Affairs; the Office of Management and Budget; the Social Security Administration; the Office of Personnel Management; the Federal

[7] *See* Executive Order 13402, Strengthening Federal Efforts to Protect Against Identity Theft (May 10, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html.

Reserve Board; the Federal Deposit Insurance Corporation; the National Credit Union Administration; the Office of the Comptroller of the Currency; the Office of Thrift Supervision; the Securities and Exchange Commission; and the United States Postal Service. Each of these agencies has a unique perspective and expertise in combating identity theft that have been invaluable to the work of the Task Force.

The Executive Order charged the Task Force with implementing the policy to use federal resources effectively "to deter, prevent, detect, investigate, proceed against, and prosecute unlawful use by persons of the identifying information of other persons," including through three specific approaches:

> (a) increased aggressive law enforcement actions designed to prevent, investigate, and prosecute identity theft crimes, recover the proceeds of such crimes, and ensure just and effective punishment of those who perpetrate identity theft;
>
> (b) improved public outreach by the federal government to better (i) educate the public about identity theft and protective measures against identity theft, and (ii) address how the private sector can take appropriate steps to protect personal data and educate the public about identity theft; and
>
> (c) increased safeguards that federal departments, agencies, and instrumentalities can implement to better secure government-held personal data.

To carry out its work, the Task Force initially organized four working level subgroups: Criminal Law Enforcement, Outreach and Prevention, Data Security (public and private sector), and Legislative and Administrative Action. All of the Task Force member agencies have worked together in close coordination to develop a coherent and comprehensive response to identity theft. In addition, the Task Force conducted extensive outreach efforts, including soliciting public comments on many of the issues under consideration by the Task Force. The public comments that we received reflected the experiences and views of consumers, identity theft victims, businesses, law enforcement officers, and many others, and will inform the Task Force's recommendations to the President.

Interim Recommendations

As I mentioned, the Task Force is still in the final stages of completing the strategic plan for presentation to the President. We anticipate that the recommendations will build on and ensure effective coordination of robust efforts already under way to prevent identity theft, to assist victims of identity theft, and to investigate and prosecute the identity thieves. We look forward to sharing those final recommendations with this Committee in the coming months. While the Task Force has been working on making final recommendations to the President, we also made some interim recommendations on September 19, 2006, on which I can report today.

The interim recommendations were intended to address steps that could be taken immediately to combat identity theft, even before the full work of the Task Force was completed. Those recommendations fall under three principal headings: prevention, victim assistance, and law enforcement. I am pleased to report that we have taken significant steps to implement these recommendations already.

Prevention

The first four interim recommendations addressed improving government handling of sensitive personal data:

Recommendation 1 involved establishing a data breach policy for the public sector. The Task Force recommended that the Office of Management and Budget (OMB) issue to all federal agencies the guidance generated by the Task Force that covers (a) the factors that should govern whether and how to give notice to affected individuals in the event of a government agency data breach that poses a risk of identity theft, and (b) the factors that should be considered in deciding whether to offer services such as free credit monitoring.

I am pleased to report that the OMB implemented this recommendation by distributing the Task Force's data breach guidance to all agencies and departments within a day of the Task Force issuing its interim recommendations. This was the first such guidance issued to federal agencies on steps to be taken in the event of a breach. We are confident that, with that guidance, agencies will be better equipped to effectively and quickly respond to data breaches and to mitigate any harms that may arise as a result of a data breach.

Recommendation 2 involved improving data security in the public sector. The Task Force recommended that OMB and the Department of Homeland Security (DHS), through the interagency effort already underway to identify ways to strengthen the ability of all agencies to identify and defend against threats, correct vulnerabilities, and manage risks: (a) outline best practices in the areas of automated tools, training, processes, and standards that would enable agencies to improve their security and privacy programs, and (b) develop a list of the top 10 or 20 "mistakes" to avoid in order to protect government information. These agencies have been working diligently on this task over the last several months, and the OMB anticipates that the resulting guidance will be issued in May 2007.

Recommendation 3 involved decreasing the use of Social Security numbers (SSNs) in the public sector. To limit the unnecessary use in the public sector of SSNs, the most valuable consumer information for identity thieves, the Task Force recommended the following:

* The Office of Personnel Management (OPM), in conjunction with other agencies, should accelerate its review of the use of SSNs in its collection of human resource data from agencies and on OPM-issued papers and electronic forms, and take steps to

eliminate, restrict, or conceal their use (including the assignment of employee identification numbers, where practicable).

* OPM should develop and issue policy guidance to the federal human capital management community on the appropriate and inappropriate use of an employee's SSN in employee records, including the proper way to restrict, conceal, or mask SSNs in employee records and human resource management information systems.

* OMB should require all federal agencies to review their use of SSNs to determine where such use can be eliminated, restricted, or concealed in agency business processes, systems, and paper and electronic forms.

This recommendation, too, is in the process of being implemented. OPM is internally conducting a review of all paper and electronic forms and taking steps to eliminate, restrict or conceal SSNs where not needed. Most of the review is complete. Some mitigation plans and activities have been completed but a large number of the actions will rely on the establishment of a Unique Employee Identifier (UEID) that will replace the SSN as the primary key in Federal employee records. OPM has conducted two agency-wide workgroup meetings to define the scope, structure, and use of the UEID, and is developing requirements and concept-of-operations documentation.

In addition, OPM is updating 5 CFR 293 to improve guidance on the restriction, concealment, and masking of SSNs in employee records and human resources information systems. The updated regulation includes comments and suggestions from a cross-agency workgroup and is currently being reviewed internally within OPM. Once completed, it will undergo the normal regulatory process.

Finally, OMB has administered a government-wide survey to assess the extent and nature of agencies' use of SSNs; identify factors to consider when determining whether use of the SSN is mission-essential and necessary to ensure program integrity or national security; and evaluate practical alternatives to use of the SSN. OMB anticipates agency review of its use of SSNs will prompt action to reduce unnecessary use and address vulnerabilities. The survey was conducted in coordination with OPM's evaluation on use of the SSN in employee records for the federal human capital management community. OMB is currently analyzing agencies' responses to the survey.

Recommendation 4 involved publication of a "routine use," under the Privacy Act, for disclosure of information following a breach. Specifically, to allow agencies to respond quickly to data breaches, including by sharing information about potentially affected individuals with other agencies and entities that can assist in the response, the Task Force recommended that all federal agencies, to the extent consistent with applicable law, publish a new "routine use" for their systems of records under the Privacy Act that would facilitate the disclosure of information in the course of responding to a breach of federal data. The Department of Justice has already

taken the lead in publishing such a routine use, and we anticipate that other agencies will soon follow.

The fifth recommendation addressed development of alternate authentication methods. Because developing reliable methods of authenticating the identities of individuals would make it harder for identity thieves to access existing accounts and open new accounts using other individuals' information, the Task Force recommended that the Task Force hold a workshop or series of workshops, involving academics, industry, and entrepreneurs, focused on developing and promoting improved means of authenticating the identities of individuals.

We are pleased to report that the first workshop will be hosted by the FTC on April 23 and 24, 2007. That public workshop, "Proof Positive: New Directions in ID Authentication," will explore methods to reduce identity theft through enhanced authentication. The workshop will facilitate a discussion among public sector, private sector, and consumer representatives, and will focus on technological and policy requirements for developing better authentication processes, including the incorporation of privacy standards and consideration of consumer usability issues. The FTC is seeking public comments in planning the agenda for the workshop, and is inviting parties interested in participating as panelists to notify the agency. The FTC is also inviting comments on ways to improve authentication processes to reduce identity theft, including, but not limited to, comments on the following questions:

- How can individuals prove their identities when establishing them in the first place?
- What are some current or emerging authentication technologies or methods -- for example, biometrics, public key infrastructure, and knowledge-based authentication -- and what are their strengths and weaknesses?
- To what extent do these technologies meet consumer needs, such as ease of use, and to what extent do they raise privacy concerns?

Victim Assistance

Recommendation 6 involved expanding the types of restitution for identity theft victims. One reason that identity theft can be so destructive to its victims is the sheer amount of time and energy often required to remediate the consequences of the offense. This may be time spent clearing credit reports with credit-reporting agencies, disputing charges with individual creditors, or monitoring credit reports for additional impacts of the theft. To allow identity theft victims to recover for the value of time they spend in attempting to remediate the harms suffered, the Task Force recommended that Congress amend the criminal restitution statutes to allow for restitution from a criminal defendant to an identity theft victim, in an amount equal to the value of time reasonably spent by the victim attempting to remediate the intended or actual harm incurred from the identity theft offense. The Department transmitted that proposed amendment to Congress on October 4, 2006. We look forward to working with this Committee to ensure that those amendments are enacted into law.

Law Enforcement

Recommendation 7 involved development of a universal police report. The Task Force recommended that the FTC and other Task Force members develop a universal police report, which an identity theft victim can complete, print, and take to any local law enforcement agency for verification and incorporation into the police department's report system. This recommendation is intended to ensure that victims can readily obtain the police reports that they need to take steps to prevent the misuse of their personal information by identity thieves, and to ensure that their complaint data are entered in a standardized format that will allow complaints to flow into a central complaint database and that thereby would assist law enforcement officers in responding to such complaints.

This recommendation, too, has been implemented. The FTC posted the standard police report form on its website in October 2006. The form is based on the online complaint form found at www.ftc.gov/idtheft, and when printed by the consumer, can be used as the basis for a police report. The FTC and others are publicizing the form's availability to law enforcement, and encouraging police departments to refer identity theft victims to the form. Use of the form should streamline the efforts for law enforcement, and enable more victims to obtain police reports, and continue their efforts to restore their good name.

* * *

In conclusion, we welcome this Subcommittee's interest in the problem of identity theft, and look forward to working with the Subcommittee and Committee in the future.

Madam Chairman, that concludes my prepared remarks. I would be pleased to take questions from you and other members of the Subcommittee.

PREPARED STATEMENT
OF

BILL WATKINS
CHIEF EXECUTIVE OFFICER

SEAGATE TECHNOLOGY, INC.
SCOTT'S VALLEY, CALIFORNIA

HEARING ON
"IDENTITY THEFT: INNOVATIVE SOLUTIONS FOR AN EVOLVING PROBLEM"

BEFORE
THE SUBCOMMITTEE ON
TERRORISM, TECHNOLOGY AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY
U.S. SENATE

March 21, 2007

Chairman Feinstein and Ranking Member Kyl:

We very much appreciate the opportunity to share with you our views about how hard disc drive full disc encryption, broadly deployed in laptop and desktop computers, can offer an innovative solution to the growing identity theft problem. As you no doubt will learn from the testimony you receive today, no one solution can solve the identity theft problem. Individuals, businesses, and the government will need to adopt a variety of best practices. By deploying advanced technology and employing common sense practices (such as using good passwords), they can substantially lessen the risk that sensitive personally identifiable information will be lost or stolen.

Seagate Technology. As the world's leading provider of hard disc drives, we know well the financial and societal risks of data loss. Last year, we shipped approximately 160 million hard disc drives, which are installed in every major PC brand purchased in the United States. We provide drives for enterprise, desktop, mobile computing, and consumer electronics applications. With approximately 54,000 employees world wide, including 2,777 at our four offices in California, we continue to grow our hard disc drive business. We have a deep appreciation for how best to protect highly sensitive data. And we share your goal of developing innovate ways of protecting sensitive personally identifiable information, such as social security numbers.

Full Disc Encryption. We are leading an industry-wide effort to develop standards for hard drive-based full disc encryption (FDE) as a way of implementing security on the hard drive, rather than through separate software. In our view, the hard drive is the ideal place to implement security for data-at-rest (that is, when a computer is turned off) because the internal operations of the drive are sealed from other elements of a computing system and the drive functions automatically to secure information without human intervention. It thus can compensate for human error.

By facilitating security of data where it is already stored, hard drive-based FDE can better protect data against theft or loss. The encryption keys are sealed and protected within the hard disc drive, are never exposed off of the drive and never appear in the clear or in any readable format on the drive. Because there is no "back door," no one except an authorized user of a device can gain access to data stored on the hard drive. A hard drive implementing full disc encryption costs about the same as software encryption sold on a licensed, per-user or per-device basis during year one and significantly less in subsequent years. (A hard drive is purchased once; by contrast, software includes an upfront cost and annual software maintenance fees.) We thus anticipate that hard drive-based FDE will become an increasingly popular means of protecting sensitive data.

Applications. Our DriveTrust™ technology can protect highly sensitive data-at-rest from theft or inadvertent disclosure. The technology can be used to make any data stored on a stolen or lost notebook unreadable and unusable *forever*. Thus, for example, if a government or corporate computer containing millions of personal records were lost or stolen, it would be nearly impossible for the thief, however sophisticated, to access the information inside the computer without knowing the password.

Although much press attention has focused on data losses involving lost or stolen computers, sensitive personal data also can be compromised when old computers are junked. Today, IT departments spend a great deal of time wiping clean existing hard drives at the end of their useful life in order to ensure sensitive data is not inadvertently compromised. Those drives often sit, unsecured, in closets awaiting destruction or "repurposing," thereby providing thieves an opportunity to steal data in an easily accessible format. Our DriveTrust™ technology can automatically repurpose existing laptops or desktops or deny access to data when computers reach the end of their useful life. There is no need to smash a drive with a hammer or to use special software to wipe it clean. By simply changing the encryption key on the disc, all stored data is instantaneously rendered unreadable and unusable forever--saving both time and money.

Recommendation. In drafting data security and identity theft legislation, the Senate Judiciary Committee should provide a safe harbor for any agency, or business entity engaged in interstate commerce, that (a) uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information and (b) deploys hard disc drive-based full disc encryption to protect it as part of a comprehensive suite of data protection efforts. By encouraging government agencies and corporate entities to invest in hard drive-based full disc encryption and to adopt common-sense practices, the Committee can substantially reduce the risk that government and corporate laptop and desktop computers will be a source of identity theft.

Thank you for considering our views.

○