PROTECTING THE PRIVACY OF SOCIAL SECURITY NUMBERS AND PREVENTING IDENTITY THEFT

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

APRIL 29, 2002

Lake Worth, Florida

Serial No. 107–71

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE

80–224 WASHINGTON : 2002

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 WAYS AND MEANS

BILL THOMAS, California, *Chairman*

PHILIP M. CRANE, Illinois
E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
AMO HOUGHTON, New York
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
JENNIFER DUNN, Washington
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
PHIL ENGLISH, Pennsylvania
WES WATKINS, Oklahoma
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY C. HULSHOF, Missouri
SCOTT MCINNIS, Colorado
RON LEWIS, Kentucky
MARK FOLEY, Florida
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ROBERT T. MATSUI, California
WILLIAM J. COYNE, Pennsylvania
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
KAREN L. THURMAN, Florida
LLOYD DOGGETT, Texas
EARL POMEROY, North Dakota

Allison Giles, *Chief of Staff*
Janice Mays, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

E. CLAY SHAW, Florida, *Chairman*

SAM JOHNSON, Texas
MAC COLLINS, Georgia
J.D. HAYWORTH, Arizona
KENNY C. HULSHOF, Missouri
RON LEWIS, Kentucky
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin

ROBERT T. MATSUI, California
LLOYD DOGGETT, Texas
BENJAMIN L. CARDIN, Maryland
EARL POMEROY, North Dakota
XAVIER BECERRA, California

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

	Page
Advisories announcing the hearing	2, 4

WITNESSES

U.S. General Accounting Office, Barbara D. Bovbjerg, Director, Education, Workforce, and Income Security Issues, accompanied by Kay Brown, Assistant Director	29
Social Security Administration, Atlanta, Georgia, Roland Maye, Special Agent-in-Charge, Atlanta Field Division, Office of Inspector General	60
Florida Office of the Attorney General, Cece Dykas	14
Florida Office of the Attorney General, 17th Judicial Circuit:	
Lee Cohen	50
Anthangtha Guialdo	51
Palm Beach County, Florida, Sheriff's Office:	
Hon. Ed Bieluch	55
Paul Rispoli	56
Tropepe, Lisa, Shalloway, Foy, Rayman & Newell Inc., accompanied by Tim Morell	7
United States Marshals Service, Anthony K. Ross	11

SUBMISSIONS FOR THE RECORD

Alpert, Maisy, Plantation, FL, letter	66
Palay, David, Las Vegas, NV, statement	66

PROTECTING THE PRIVACY OF SOCIAL SECURITY NUMBERS AND PREVENTING IDENTITY THEFT

MONDAY, APRIL 29, 2002

HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Lake Worth, Florida.

The Subcommittee met, pursuant to notice, at 2:15 p.m., in Commission Chambers, Lake Worth City Hall, Lake Worth, Florida, Hon. E. Clay Shaw, Jr., (Chairman of the Subcommittee) presiding.

[The advisory and revised advisory follow:]

ADVISORY

COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
April 22, 2002
No. SS–13

Contact: (202) 225–9263

Shaw Announces Hearing on Social Security Protecting the Privacy of Social Security Numbers and Preventing Identity Theft

Congressman E. Clay Shaw, Jr. (R–FL), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a field hearing on protecting the privacy of Social Security numbers (SSNs) and preventing identity theft. **The hearing will take place on Monday, April 29, 2002, in the Commission Chambers, Lake Worth City Hall, 7 North Dixie Highway, Lake Worth, Florida, beginning at 1:00 p.m.**

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Subcommittee and for inclusion in the printed record of the hearing.

BACKGROUND:

The SSN was created in 1936 for the sole purpose of tracking workers' Social Security earnings records. Today, SSN use has expanded well beyond its original purpose. According to the Social Security Administration (SSA), the SSN is the single-most widely used record identifier in the public and private sectors. Federal law requires the use of SSNs for administration of income taxes, the Food Stamp, Medicaid, and other Federal programs. In the private sector, SSNs are commonly used for record-keeping and data exchange systems, and often businesses require individuals to disclose their SSN as a condition for doing business.

Many believe widespread use of the SSN benefits the public by improving access to financial and credit services in a timely manner, reducing administrative costs, and improving record keeping so consumers can be contacted and identified accurately. Others argue the pervasive use of SSNs makes them a primary target for fraud and misuse. Most recently, the events of September 11 have shed new light on the severe consequences of failure to protect the integrity of SSNs, as the ensuing investigations have exposed the methods used by the terrorists who assumed false identities to carry out their activities.

In addition to being a gateway to terrorist acts, identity theft causes misery and frustration in the daily lives of tens of thousands of Americans. Identity theft is the number one consumer complaint received by the Federal Trade Commission, amounting to 42 percent of complaints received in 2001. In a recent report, the U. S. General Accounting Office found that identity theft appears to be growing (Identity Theft—Prevalence and Cost Appear to Be Growing: GAO–02–363). Report findings include: (1) the SSA Office of Inspector General has reported a substantial increase in call-ins of identity theft-related allegations to its Fraud Hotline, where allegations involving SSN misuse (81 percent of which relate directly to identity theft) have increased more than fivefold (11,000 to 65,000) in the 4 years ending September 2001; (2) seven-year fraud alerts (warnings to credit grantors to conduct additional identity verification before granting credit) have increased substantially (36 percent and 53 percent respectively) in the last 3 years, according to two consumer

reporting agencies; and, (3) in its 2000 annual report, the Postal Service indicated that investigations of identity theft crime increased by 67 percent since the previous year.

To increase the privacy of SSNs and better protect the American public from being victimized, Chairman Shaw, along with several Members of the Committee on Ways and Means, introduced bipartisan legislation, H.R. 2036, the "Social Security Number Privacy and Identity Theft Prevention Act of 2001." This legislation prohibits the sale and display of SSNs by Federal, State, and local governments, prohibits the sale of SSNs by the private sector, deters businesses from denying services when someone refuses to provide the SSN, and increases fines and penalties for SSN misuse.

In announcing the hearing, Chairman Shaw stated: "Although never created to be a personal identifier, the use of SSNs is now pervasive throughout our automated society. As highlighted by the September 11 attacks, these numbers are far too easily used by criminals or terrorists to steal identities and obtain false documents. The ravages of SSN misuse are experienced by each and every victim of identity theft and now by our Nation through their role in facilitating terror. We must act to take whatever steps we can to protect the privacy of each and every Americans' SSNs. It's the right thing to do and a necessary step in our Nation's response to terrorism."

FOCUS OF THE HEARING:

The hearing will focus on what victims experience when their identities are stolen, the challenges law enforcement faces as they pursue identity thieves, the use of SSNs by government agencies at the Federal, State, and local levels, practices used to safeguard privacy, and the impact of legislative proposals aimed at combating SSN misuse and protecting privacy.

DETAILS FOR SUBMISSIONS OF WRITTEN COMMENTS:

Please Note: Due to the change in House mail policy, any person or organization wishing to submit a written statement for the printed record of the hearing should send it electronically to *hearingclerks.waysandmeans@mail.house.gov*, along with a fax copy to (202) 225–2610, by the close of business, Monday, May 13, 2002. Those filing written statements who wish to have their statements distributed to the press and interested public at the hearing should deliver 200 copies to the West Palm Beach District Office of Congressman E. Clay Shaw, Jr., 222 Lakeview Avenue, Suite 162, West Palm Beach, Florida 33401, by the close of business, Friday, April 26, 2002.

FORMATTING REQUIREMENTS:

Each statement presented for printing to the Committee by a witness, any written statement or exhibit submitted for the printed record or any written comments in response to a request for written comments must conform to the guidelines listed below. Any statement or exhibit not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. Due to the change in House mail policy, all statements and any accompanying exhibits for printing must be submitted electronically to *hearingclerks.waysandmeans@mail.house.gov*, along with a fax copy to (202) 225–2610, in Word Perfect or MS Word format and MUST NOT exceed a total of 10 pages including attachments. Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. Any statements must include a list of all clients, persons, or organizations on whose behalf the witness appears. A supplemental sheet must accompany each statement listing the name, company, address, telephone and fax numbers of each witness.

Note: All Committee advisories and news releases are available on the World Wide Web at *http://waysandmeans.house.gov/*.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call (202) 225–1721 or (202) 226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

*****NOTICE—CHANGE IN TIME*****

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
April 25, 2002
No. SS–13–Revised

Contact: (202) 225–9263

Change in Time for Subcommittee Field Hearing on Protecting the Privacy of Social Security Numbers and Preventing Identity Theft

Congressman E. Clay Shaw, Jr. (R–FL), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee field hearing on Protecting the Privacy of Social Security Numbers and Preventing Identity Theft, scheduled for Monday, April 29, 2002, at 1:00 p.m., in the Commission Chambers, Lake Worth City Hall, 7 North Dixie Highway, Lake Worth, Florida, **will now be held at 2:00 p.m.**

All other details for the hearing remain the same. (See Subcommittee Advisory **No. SS–13**, dated April 22, 2002.)

Chairman SHAW. We will call the hearing to order. This is about Social Security Numbers (SSNs), and although they were created solely for the purpose of tracking workers' Social Security earnings, our culture is hooked on Social Security Numbers. Even the most trivial transactions require us to hand over our nine-digit ID before services can be rendered.

I phoned in just this weekend to renew my fishing license, and they wanted my Social Security Number, the State of Florida. I said, "Is it required?" They said, "No, but it would be nice if you give it." And I said, "I don't believe I will." So they took my driver's license number instead.

Our Social Security Number's the key that unlocks the door to your identity for any unscrupulous individual who gains access to it. Once the door is unlocked, the criminal or terrorist has at his fingertips all essential elements needed to carry out whatever das-

tardly act they can conceive of. Worse, we know that some terrorists involved on the September 11 attack illegally obtained Social Security Numbers and used them to steal identities and obtain false documents, thus enabling them to live within our borders and plan their heinous acts. government and private industry must be vigilant to protect our identities. Safeguards to protect Social Security Numbers and prevent identity theft must be put in place now.

As a first step, I, along with several of my Committee on Ways and Means colleagues, including Mark Foley, introduced bipartisan legislation entitled, the Social Security Number Privacy and Identity Theft Prevention Act. The bill prohibits the sale and display of Social Security Numbers by Federal, State and local governments and restricts the sale and display of Social Security Numbers by the private sector and deters business from denying services when someone refuses to provide their number and increase fines and penalties for Social Security Number misuse.

Today, we will shine a bright light on the need to quickly bring comprehensive legislation to the House floor to keep Social Security Numbers private and protect citizens from identity theft. The time for action is long overdue.

Field hearings allow us the unique opportunity to get out of Washington and hear the real-life experience of our neighbors on the frontlines of these important issues. I sincerely want to thank the City of Lake Worth for allowing us to hold this hearing in the Commission Chambers.

[The opening statement of Chairman Shaw follows:]

Opening Statement of the Hon. E. Clay Shaw, Jr., a Representative in Congress from the State of Florida, and Chairman, Subcommittee on Social Security

Although created solely for the purpose of tracking workers' Social Security earnings, our culture is hooked on Social Security numbers. Even the most trivial transactions require us to hand over our 9-digit ID before services can be rendered.

Your Social Security number is the key that unlocks the door to your identity for any unscrupulous individual who gains access to it. Once the door is unlocked, the criminal or terrorist has at their fingertips all the essential elements needed to carry out whatever dastardly act they can conceive.

Worse, we know that some terrorists involved in the September 11th attacks illegally obtained Social Security numbers and used them to steal identities and obtain false documents, thus enabling them to live within our borders and plan their heinous crimes.

Government and private industry must be vigilant in protecting identities. Safeguards to protect Social Security numbers and prevent identity theft must be put in place now.

As a first step, I, along with several of my Ways and Means colleagues introduced bipartisan legislation, the *Social Security Number Privacy and Identity Theft Prevention Act*. This bill prohibits the sale and display of Social Security numbers by Federal, State and local governments, restricts the sale and display of Social Security numbers by the private sector, deters businesses from denying services when someone refuses to provide their number, and increases fines and penalties for Social Security number misuse.

Today we will shine a bright light on the need to quickly bring comprehensive legislation to the House floor to keep Social Security numbers private and protect citizens from identity theft. The time for action is long overdue.

Field hearings allow us the unique opportunity to get out of Washington and hear the real life experiences of our neighbors on the front lines of this important issue. I sincerely thank the City of Lake Forth for allowing us to hold this hearing in the Commission Chambers.

Today, we welcome a neighbor and a former neighbor, Ms. Tropepe and Mr. Ross, who will share their personal stories about the theft of their identities. In addition,

Barbara Bovberg of the General Accounting office will discuss government use of Social Security numbers.

We will also hear about the many challenges faced by the law enforcement community as they hunt down identity thieves. We welcome Cece Dykas of the Office of the Attorney General; Lee Cohen of the State Attorney's Office, the Sheriff of Palm Beach County, Sheriff Ed Bieluch; and Roland Maye of the Social Security Administration's Office of Inspector General.

Welcome to all.

Chairman SHAW. Mark, I believe your political life started right here in this building.

Mr. FOLEY. In this very seat.

Chairman SHAW. Oh. Today we welcome a neighbor and former neighbor, Mrs. Tropepe and Mr. Ross, who will share their personal stories about the theft of their identities. In addition, Barbara Bovbjerg of the U.S. General Accounting Office will discuss government use of Social Security Numbers. We will also hear about the many challenges faced by law enforcement as they hunt down identity theft. We want to welcome representatives from the Office of the Attorney General, the State's Attorney's Office, we have the Sheriff of Palm Beach County, and we have also Mr. Maye of the Social Security Administration (SSA), Office of the Inspector General (OIG). I want to welcome all of you, and I will, at this time, yield to Mr. Foley for any comments that he might have.

Mr. FOLEY. Thank you very much, Clay. And, first, let me thank everybody. It is a delight and honor to be back in this seat, in this city, in the first political office I ever held, and I think longingly of those days when life was easy and we didn't have the problems we have today.

I am particularly pleased to see the number of panelists here. And, Lisa, specifically, thank you for joining us. You mentioned to me a few weeks ago the problems you had, and it was interesting because I had relayed a similar problem that I had where somebody took my Social Security Number and applied for credit. I got the first notice from Target Collection Agency that I had somehow charged $780 worth of goods and services. We got a copy of the application for credit. It showed my Social Security Number, said the person worked for the government. The only thing different was they used an address, Powerline Boulevard in Pompano Beach, Florida. So everything else they had on me. Target extended credit. That person walked away with $700-plus merchandise. I spent countless hours trying to reconcile this issue. It was horrific, and I felt if I had to go through so much trouble, imagine someone who may not have a phone that is able to reach during the day, who may not have the tenacity, who may be a single mother having to deal with kids and family all day long and then hustle up to try and see if they can get these collection agencies off their phones and off their backs. I felt violated. I couldn't believe it could occur, but as Congressman Shaw suggested, it is happening far too frequently.

I want to thank my colleague, because he had the bill long before I came involved with this, but when I heard the subject matter of the bill, I told him of my own experience and enthusiastically wanted to jump on board to see whatever we could do to eliminate this

kind of problem, because it is, it is a sad commentary, it is a tragedy when you have to go through it, and so I joined together with my colleague hopefully getting something done on this issue. And thank you, Clay, for coming to Lake Worth—your district, my old hometown.

Chairman SHAW. Thank you, Mark. Our first panel—we will have two panels today. The first panel, Lisa Tropepe, who is the Partner at Shalloway, Foy, Rayman & Newell, Incorporated, West Palm Beach, Florida; accompanied by Tim Morell, attorney, West Palm Beach, Florida; Anthony Ross, who is a Federal Law Enforcement Officer, United States Marshals Service in Brunswick, Georgia; Cece Dykas, who is the Assistant Deputy Attorney General, Florida Office of the Attorney General, Palm Beach County; and Barbara Bovbjerg who is the Director of Education, Work force and Income Security Issues, the U.S. General Accounting Office from Washington. She often appears before us in Washington. And Kay Brown, Assistant Director of Education, Work force and Income Security Issues, the U.S. General Accounting Office, also in Washington.

From each one of you we have, I believe for all, if not most of you, your written statements which will be made a part of the record. You may proceed as you see fit.

Lisa?

STATEMENT OF LISA A. TROPEPE, PARTNER, SHALLOWAY, FOY, RAYMAN & NEWELL, INC., WEST PALM BEACH, FLORIDA, ACCOMPANIED BY TIM MORELL, ATTORNEY

Ms. TROPEPE. Thank you. For the record, I just wanted to let you know that Tim Morell is my attorney. My firm and I had to hire him when this was happening to me, and he is here on my behalf.

Dear Committee Members, good afternoon. My name is Lisa A. Tropepe, and I have been a victim of identity theft. I am beginning my testimony with a copy of a May 7, 1999, letter to Judge Oftedahl articulating the seriousness of the crimes against me and the importance of penalizing the imposter for all the crimes committed. The letter is dated May 7, 1999. It is in reference to the State of Florida v. Terkesha L. Lane.

"Dear Judge Oftedahl, Assistant State Attorney Chris Jette called to let me know that Terkesha L. Lane is scheduled for arraignment today. The crime against me was that the defendant, while working as a temporary receptionist at my office stole personal information about me and assumed my identity. She cleaned out my personal bank account and opened several credit card accounts where she charged up to thousands of dollars of merchandise.

Although I was initially advised by intake officer Brian Brennan, Esq., that the defendant would be charged with multiple counts of grand theft and counts relating to the fraudulent assumption of my identity, I am now advised that only one charge of theft has been made. My employers and I are concerned that the courts may not be well advised as to the personal seriousness and public danger this crime represents.

With those thoughts in mind, I feel compelled to write this letter in the hope of informing you of the impact of the crime of identity theft that was perpetrated upon me and, indirectly upon my firm by Ms. Lane.

This person stole approximately $20,000 from credit grantors and my personal bank account using my name. She applied and received a valid driver's license with her picture and my name, address, and so forth., on the license. She subsequently applied for credit cards, received temporary credit limits, and spent accordingly. She also entered my bank several times and withdrew $13,900 from my personal bank account. Now I am spending hundreds of frustrating hours dealing by phone and letters with collection companies, banks, credit reporting agencies, governmental agencies, (Division of Highway Safety and Motor Vehicles, Postal authorities, Social Security, etc.) and various other companies to convince them of the fraud, and to clean up the disaster affecting my credit and other aspects of my finances.

The out-of-pocket costs are substantial. However, far more devastating is learning that someone has invaded every aspect of my life and taken my identity. My credit is ruined, my good reputation is stolen and tarnished, my career and livelihood has been impaired, and I am subjected to possible further invasion in the future.

I will briefly outline several aspects of this nightmare.

My office and I have spent over 100 hours calling, filling out documentation, writing letters return receipt requested to banks, credit reporting agencies, governmental agencies, companies, utilities, credit grantors, etc., to inform them of the fraud in an attempt to prove my own innocence. The burden is on the victim to prove fraud since there is great suspicion by the credit grantors. In fact, since I put fraud alerts and new passwords on all my accounts, I have experienced extensive questioning and delays in dealing with the various banks and agencies. I am told by the Privacy Rights Clearinghouse and the Federal Trade Commission that my problems may go on for several years.

This has been a very frightening and invasive nightmare. I have had great difficulty sleeping and have woken in cold sweats worrying about what else I will find out. The impersonator was a temporary employee at my office. She was our temporary receptionist in charge of outgoing mail and phone messages. When I realized someone had taken my identity and was applying for credit cards in my name, I shared my problem with her. She subsequently hugged me and said everything will be okay. She never wavered in her demeanor. I truly believed that she was concerned. I was shocked to see her caught on tape withdrawing money from my bank account.

I have had nightmares seeing the defendant invading my home and hurting me physically. She lives in Riviera Beach, and I live in Palm Beach Shores (Singer Island), which is only 5 minutes away. She knows where I live.

Stealing my identity has made me feel very vulnerable and violated. It has been stressful and literally made me ill. I do not like to think of myself as a victim. I am a professional engineer and am responsible for multi-million dollar projects, handling many com-

plex problems related to the health, safety and welfare of the public. Because of this, I thought at first that I could handle this stress without any help. However, I found it so overwhelming that I had to hire an attorney and am in the process of scheduling a meeting with a therapist.

I respectfully request that Your Honor consider the serious nature of these crimes.

I believe this defendant and other wrongdoers who might see this as an easy crime to commit with potentially big money to steal and no real punishment to face, learn that society will not tolerate this type of insidious crime. For that reason, I strongly urge that she experience jail time, not just a couple of months on probation.

I am concerned about of what she will do to me in the future. I trust you take this crime seriously. In that connection, I am also concerned that the charges being brought against this wrongdoer don't include charges for credit card theft and fraud under Florida Statute 817.

Thank you for your consideration. Sincerely, Lisa A. Tropepe."

It has been almost exactly 3 years since I sent the above May 7, 1999, letter to Judge Oftedahl. In 3 years, the following has occurred. One, Turkesha L. Lane never served a day in prison. Turkesha L. Lane still has my Social Security Number, my home address and workplace. If she has not moved, Turkesha L. Lane still lives 5 minutes away from my home. Two, my credit record will never be the same. Perpetual fraud alerts and annual credit bureau inquiries have been, and will be, a part of my life for the rest of my life. Three, a reoccurrence is always in the back of my mind. After 3 years, I still shutter at the thought of someone impersonating me. My summation of this incident can only be described in two words: electronic rape.

A part of me wants to thank you for giving me this opportunity to share my experience with all of you. However, a part of me is fearful that my testimony may call attention to other criminals regarding my vulnerability to be impersonated again. As lawmakers, I trust that you will provide the necessary laws needed to stop this awful crime.

[The prepared statement of Ms. Tropepe follows:]

Statement of Lisa A. Tropepe, Partner, Shalloway, Foy, Rayman & Newell Inc., West Palm Beach, Florida

Dear Committee Members:

Good Afternoon, my name is Lisa A. Tropepe and I have been a victim of identity theft. I am beginning my testimony with a copy of a May 7, 1999 letter to Judge Oftedahl articulating the seriousness of the crimes against me and the importance of penalizing the imposter for all the crimes committed.

May 7, 1999

The Honorable Richard L. Oftedahl,
Room 11.2213, Division X
Palm Beach County Courthouse,
205 N. Dixie Highway,
West Palm Beach, FL 33401

IN RE: State of Florida v. Terkesha L. Lane; *PBSO #99–053521; Assigned to Assistant State Attorney Chris Jette, Division X; Arrainment date 5/7/99*

Hand Delivered

Dear Judge Oftedahl:

Assistant State Attorney Chris Jette called to let me know that Terkesha L. Lane is scheduled for arraignment today. The crime against me was that the defendant while working as a temporary receptionist at my office stole personal information about me and assumed my identity. She cleaned out my personal bank account and opened several credit card accounts where she charged up thousands of dollars of merchandise.

Although I was initially advised by intake officer Brian Brennan, Esq., that the defendant would be charged with multiple counts of grand theft and counts relating to the fraudulent assumption of my identity, I am now advised that only one charge of theft has been made. My employers and I are concerned that the courts may not be well advised as to the personal seriousness and public danger this crime represents.

With those thoughts in mind, I feel compelled to write this letter in the hope of informing you of the impact of the crime of identity theft that was perpetrated upon me and, indirectly upon my firm, by Ms. Lane.

This person stole approximately $20,000.00 from credit grantors and my personal bank account using my name. She applied and received a valid driver's license with her picture and my name, address, etc., on the license. She subsequently applied for credit cards, received temporary credit limits, and spent accordingly. She also entered my bank several times and withdrew $13,900.00 from my personal bank account. Now I am spending hundreds of frustrating hours dealing by phone and letters with collection companies, banks, credit reporting agencies, governmental agencies, (Division of Highway Safety and Motor Vehicles, Postal authorities, Social Security, etc.) and various other companies to convince them of the fraud, and to clean up the disaster affecting my credit and other aspects of my finances.

The out-of-pocket costs are substantial. However, far more devastating is learning that someone has invaded every aspect of my life and taken my identity. My credit is ruined, my good reputation is stolen and tarnished, my career and livelihood has been impaired, and I am subjected to possible further invasion in the future.

I will briefly outline several aspects of this nightmare:

My office and I have spent over 100 hours calling, filling out documentation, writing letters return receipt requested to banks, credit reporting agencies, governmental agencies, companies, utilities, credit grantors, etc. to inform them of the fraud in an attempt to prove my own innocence. The burden is on the victim to prove fraud since there is great suspicion by the credit grantors. In fact, since I put fraud alerts and new passwords on all my accounts, I have experienced extensive questioning and delays in dealing with the various banks and agencies. I am told by the Privacy Rights Clearinghouse and the Federal Trade Commission that my problems may go on for several years. **See articles attached—including an article from Wednesday's Sun Sentinel which reports a nearly identical case.**

This has been a very frightening and invasive nightmare. I have had great difficulty sleeping and have awoken in cold sweats worrying about what else I will find out. The impersonator was a temporary employee at my office. She was our temporary receptionist in charge of outgoing mail and phone messages. When I realized someone had taken my identity and was applying for credit cards in my name, I shared my problem with her. She subsequently hugged me and said everything will be okay. She never waivered in her demeanor. I truly believed that she was concerned. I was shocked to see her caught on tape withdrawing money from my account.

I have had nightmares seeing the defendant invading my home and hurting me physically. She lives in Riviera Beach and I live in Palm Beach Shores (Singer Island), which is only five minutes away. **She knows where I live.**

Stealing my identity has made me feel very vulnerable and violated. It has been stressful and literally made me ill. I do not like to think of myself as a victim. I am a professional engineer and am responsible for multi-million dollar projects, handling many complex problems related to the health, safety and welfare of the public.

Because of this, I thought at first that I could handle this stress without any help. However, I found it so overwhelming that I had to hire an attorney and am in the process of scheduling a meeting with a therapist.

I respectfully request that Your Honor consider the serious nature of these crimes.

I believe this defendant and other wrongdoers who might see this as an easy crime to commit with potentially big money to steal and no real punishment to face, learn that society will not tolerate this type of insidious crime. For that reason, I strongly urge that she experience jail time, not just a couple months on probation.

I am concerned about of what she will do to me in the future. I trust you take this crime seriously. In that connection, I am also concerned that the charges being brought against this wrongdoer don't include charges for credit card theft and fraud under Florida Statute 817.

Thank you for your consideration.

Sincerely,

Lisa A. Tropepe

It has been almost exactly three years since I sent the above May 7, 1999 letter to Judge Oftedahl. In the three years the following has occurred:

1. Terkesha L. Lane never served a day in prison. Terkesha L. Lane still has my social security number, my home address and workplace. If she has not moved, Terkesha L. Lane still lives five minutes away from my home.

2. My credit record will never be the same. Perpetual fraud alerts and annual Credit Bureau inquiries have been and will be a part of my life for the rest of my life.

3. A reoccurrence is always in the back of my mind. After 3 years I still shutter at the thought of someone impersonating me. My summation of this incident can only be described in two words—"Electronic Rape".

A part of me wants to thank you for giving me this opportunity to share my experience with all of you. However, a part of me is fearful that my testimonial may call attention to other criminals regarding my vulnerability to be impersonated again. As lawmakers, I trust that you will provide the necessary laws needed to stop this awful crime.

Chairman SHAW. Thank you for that testimony. I think we are all vulnerable. Mr. Ross?

STATEMENT OF ANTHONY K. ROSS, FEDERAL LAW ENFORCEMENT OFFICER, UNITED STATES MARSHALS SERVICE, BRUNSWICK, GEORGIA

Mr. ROSS. Thank you. Good afternoon. My name is Anthony Ross, and I would like to thank the Honorable Clay Shaw, Social Security Subcommittee and the Social Security Administration Office of Inspector General for inviting me to testify to you today.

The illegal use of another's identity is a serious problem costing the American taxpayers and businesses billions of dollars. Additionally, it destroys the credit of a very large number of citizens daily. I am one of those citizens and also a Federal Law Enforcement Officer, the United States Marshals Service.

In April 2000, I became aware that I was a victim of identity theft when contacted by my banking institution. In a few days time, a person had assumed a false Florida driver's license with my name and information, cashed five checks for $995 each. I went through a few weeks of closing accounts and then finding that my accounts were now frozen and the moneys transferred back to the original accounts. This occurred several times during approximately a 2-week period. Eventually, it was resolved when out of

frustration I closed all the accounts and began banking with another institution.

Shortly thereafter, I was going to purchase a home subsequent to relocating from Florida to Georgia. The mortgage institution ran a credit check and inquired I had opened more than 25 revolving credit accounts in approximately a month's time. SunTrust was very professional, and they were quick in determining that I was not the cause of these accounts, and the purchase of my home went through without difficulty.

However, from that point on it has been a nightmare and that is because my identity was illegally used to obtain in excess of $50,000 worth of credit charges. I have contacted credit bureaus and established flags for being a victim of identity theft. I have contacted numerous credit card companies, spending extended lengths of time just trying to get through the computerized phone systems, and then to a living person and then transferred again to reach a person in the Fraud Investigations Department. I have struggled with trying to read or more likely decipher credit reports; they are not user-friendly.

I have contacted numerous creditors and filled out endless forms, filed affidavits, provided copies of driver's license, Social Security card to try to prove my innocence. That is right, the victim has to prove he is innocent. In many cases, I have received letters indicating that I have been cleared and credit bureaus that have been notified. However, and this is after looking up my most recent credit reports, the credit bureaus have not properly disclosed that information on my credit report.

In June 2000, I received a Notice of Court appearance to answer for charges regarding failure to redeliver a hired vehicle. Again, my identity information was misused, and now I face the possibility of being arrested. At the least, I was now, as a Law Enforcement Officer, on the wrong end of the judicial system. Again, I had to prove my innocence by providing photographs and fingerprint cards. Metro-Dade Police Identity Unit was very professional and prompt in assisting me with clearing up this situation, as well as the State Attorney's Office.

During this ordeal, I attempted to get assistance through several law enforcement agencies. I would call and get transferred, received voice mail, and then when I did speak to a detective I was generally given very little positive indication that anything would be done other than establish a crime report. Some law enforcement indicated they were very overwhelmed with identity theft activity, and I was part of a long list.

Due to the abundance of identity theft and limited law enforcement resources, proper attention to my case was initially very poor. And that was until I contacted Special Agent Ray Llorca of the Social Security Administration. Special Agent Llorca promptly scheduled a meeting with me and obtained information and statements from me, and he was permitted to open an investigation. As a result, I testified in a State grand jury in July 2001. I was informed that six people were indicted in this scheme regarding identity theft and credit card/banking fraud.

As recently as March 2002, a collection agency provided me an offer to settle an account with a balance of over $4,000, and this

was for a substantially reduced amount. They were actually going to let me make two payments for about, oh, $1,200 and change each. What a deal, okay? This was in regards to an account that was illegally opened using my identity. A recent credit report indicates that I have 38 serious delinquency in public record or collections filed, none of which are truly my responsibility, but I must deal with them until they are cleared.

The point I am trying to make is that even after crime, the investigation and to some extent the judicial proceedings, we, as victims of identity theft, are still trying to clear our names and restore our credit. Thank you.

[The prepared statement of Mr. Ross follows:]

Statement of Anthony Ross, Federal Law Enforcement Officer, United States Marshals Service, Brunswick, Georgia

Good Afternoon, my name is Anthony Ross.

I would like to thank the Honorable Clay Shaw, Social Security Subcommittee and the Social Security Administration Office of Inspector General for inviting me to testify to you today.

The illegal use of another's identity is a serious problem costing American taxpayers and businesses billions of dollars. Additionally, it destroys the credit of very large number of citizens daily. I am one of those citizens and also a Federal Law Enforcement Officer with the United States Marshals Service.

In April of 2000 I became aware that I was a victim of identity theft when contacted by my banking institution. In a few days time a person assumed a false Florida Drivers License and cashed five checks for $995.00 each. I went through a few weeks of closing accounts and then finding that my accounts were frozen and monies transferred back to the original accounts. This occurred several times in that time period. Eventually it was resolved when out of frustration, I closed all accounts and began business with another banking institution.

Shortly thereafter, I was going to purchase a home subsequent to relocating from Florida to Georgia. The mortgage institution ran a credit check and inquired if I had opened more than 25 revolving credit accounts in approximately a month's time. Sun Trust was very professional and quick in determining that I was not the cause of these credit problems. The purchase of the home went through without difficulty.

However, from that point on it has been a nightmare. That's because my identity was illegally used to obtain in excess of $50,000.00 worth of credit charges. I have contacted credit bureaus and established flags for being a victim of identity theft. I have contacted numerous credit card companies spending extended lengths of time just trying to get through the computerized phone systems and then to a living person and then transferred again to reach a person in a fraud investigations department. I have struggled with trying to read or more likely decipher credit reports. They are not consumer friendly. I have contacted numerous creditors and have filled out endless forms, filed affidavits, provided copies of Drivers License and Social Security card to try to prove my innocence. That's right, the victim has to prove he is innocent. In many cases, I received letters indicating that I have been cleared and credit bureaus notified. However, In some cases that has not been properly disclosed on my credit report.

In June of 2000 I received a Notice of Court appearance to answer for charges regarding Failure to Redeliver a Hired Vehicle. Again, my identity information was misused and now I faced the possibility of being arrested. At the least, I was now seen as a law enforcement officer on the wrong end of the judicial system. Again, I had to prove my innocence by providing photos and fingerprint cards. Metro-Dade Police Identity Unit was very professional and prompt in assisting with clearing up this situation as well as the State Attorney's Office.

During this ordeal, I attempted to get assistance through several law enforcement agencies. I would call and get transferred and receive voice mail. When I did speak to a Detective, I was given very little positive indication that anything would be done other than establishing a crime report. Some law enforcement indicated they were overwhelmed with identity theft activity and I was part of a long list. Due to the abundance of identity theft, and limited law enforcement resources, proper attention to my case was initially very poor. That was until I contacted Special Agent Ray Llorca of the Social Security Administration, Office of Inspector General. S/A Llorca promptly scheduled a meeting with me and obtained information and state-

ments and was permitted to open an investigation. As a result, I testified in a State Grand Jury in July 2001 and I was informed that six people were indicted in this scheme regarding identity theft and credit card/banking fraud.

As recently as March 2002, a collection agency provided me an offer to settle an account with a balance of over $4000.00 for a substantially reduced amount. What a deal! This was in regards to an account that was illegally opened using my identity. A recent credit report indicates that I have 38 serious delinquency and public record or collections filed. None of which are truly my responsibilities, but I must deal with them until they are cleared.

The point I am trying to make is that even after crime, the investigation, and to some extent, the judicial proceedings, we as victims of identity theft are still trying to clear our names and restore our credit.

Thank you.

Chairman SHAW. Mr. Dykas?

STATEMENT OF CECE DYKAS, ASSISTANT DEPUTY ATTORNEY GENERAL, FLORIDA OFFICE OF THE ATTORNEY GENERAL, PALM BEACH COUNTY OFFICE, FT. LAUDERDALE, FLORIDA

Mr. DYKAS. Good afternoon, Chairman, Congressman Foley. My name is Cece Dykas. I am the Assistant Deputy Attorney General for south Florida. Unfortunately, Florida finds itself on the forefront of identity theft issues, but hopefully we will also be on the forefront, along with the Federal Government, in trying to help stop these. In 1999, the Governor requested a Privacy and Technology Task Force. As a result of that task force and the testimony that was generated from that, a State grand jury was empanelled to deal with the variety of issues, including identity theft, along with the theft of driver's licenses.

The grand jury that was empanelled recently released their report in January 10, 2002. To date, there have been at least 56 defendants who have been charged with over 470 counts. There is a projected loss for the year 2005 that there will be a theft of $8 billion. They estimate that the average loss per person in an identity theft scheme is $17,000, as the other panelists, just through their own experience, have indicated. The average length of time between a theft occurring and a victim finding out that their identity has been stolen is generally 12.7 months. The average victim spends up to at least 3 months and over $800 of their money to try and clear their name.

Your Social Security, as the Chairman indicated when he was getting his fishing license, is on virtually everything. It is doctors' offices, video rentals, school applications. As a result of that, the Florida legislature, in the past several years, have passed Statutory section 817.568, Subsection 8. It allows for the prosecution of identity theft based on the residency of the victim. In many ways, part of the problem in prosecuting identity theft was to be able to determine where the crime had occurred. That statute now allows for the place of resident of the victim to determine jurisdiction.

One of the recommendations or several of the recommendations of the task force were that they be established a nationally recognized identity theft prosecution unit within the Office of statewide Prosecution, that there be a devotion of resources for the training of Florida prosecutors and law enforcement officers on issues related to the investigation and prosecution of identity theft, that the

legislation appropriation of funds to study and report on design methods and procedures to make the Florida drivers' licenses and identification card more resistant to tampering and counterfeiting. There is also a request for a formation for a multi-disciplined focus group to study security features of the Florida driver's license and identification card to make it one of the most secure driver's licenses and ID cards in the country.

This past session, or should I say current session, that is going on in Tallahassee, has several bills before it dealing specifically with the issue of identity theft. Senate bill 140 criminalizes the use of any public record to commit a further crime. House bill 1673 makes Social Security Numbers in the hands of State agencies exempt from disclosure under chapter 119. House bill 1675 exempts bank account numbers or credit card charge or debit account numbers in the hands of State agencies from disclosure under chapter 119.

House bill 1679 sets up a study commission on how the State treats personal ID information in public hands, whether excessive or unnecessary information is collected. The impact of advanced technologies on full access to public records, whether to treat the public access to physical documents differently than public access to electronic documents and other issues that underline the balance between the two. Senate bill 1020, and the bill makes a non-criminal violation for merchants who accept payment by electronic payment cards to leave more than the last five digits of the customer's account number showing on any receipt.

And, finally, Senate bill 520, which provides an infrastructure and raises the standards for issuance of driver's license. It provides that a breeder document, those used to prove the identify of the applicant, be preserved by the Department, makes reciprocity and accepting out-of-State driver's licenses contingent on the other State having adopted standards as stringent as Florida's and provides that any driver's licenses used to a foreign national will not be valid for longer than a 2-year period of time.

Presently, those bills are before the legislature and have bipartisan support, so hopefully those will be passed this session. Thank you very much.

[The prepared statement of Mr. Dykas follows:]

Statement of Cece Dykas, Assistant Deputy Attorney General, Florida Office of the Attorney General, Palm Beach County Office, Ft. Lauderdale, Florida

What is ID Fraud?

- Involves the use of personal identifying information to commit fraud
- Can range from unauthorized use of a credit card to a comprehensive takeover of another person's identity
- Can result in the loss of assets or creditworthiness
- Criminalized in Florida by §817.568 Florida Statutes

Scope of the Problem

- ID Fraud can claim many victims, including credit grantors and the individuals whose identities are stolen.
- Visa USA, Inc., indicated that fraud losses related to ID Fraud totaled $490 million in 1997.
- Mastercard, Inc., indicated that fraud losses related to ID Fraud totaled $407 million in 1997.

Scope of the Problem

- ID Fraud is probably the fastest growing crime in the country
  - not new but technology has streamlined the process
  - vast amounts of information readily available
  - able to secure credit and goods instantaneously through the Internet

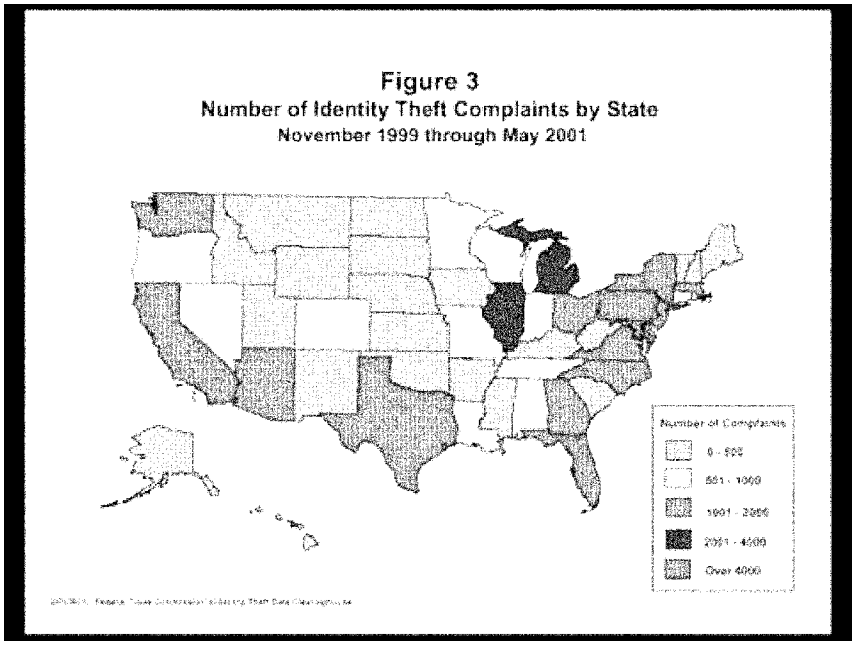


Figure 3
Number of Identity Theft Complaints by State
November 1999 through May 2001
Number of Complaints
0 - 500
501 - 1000
1001 - 2000
2001 - 4000
Over 4000

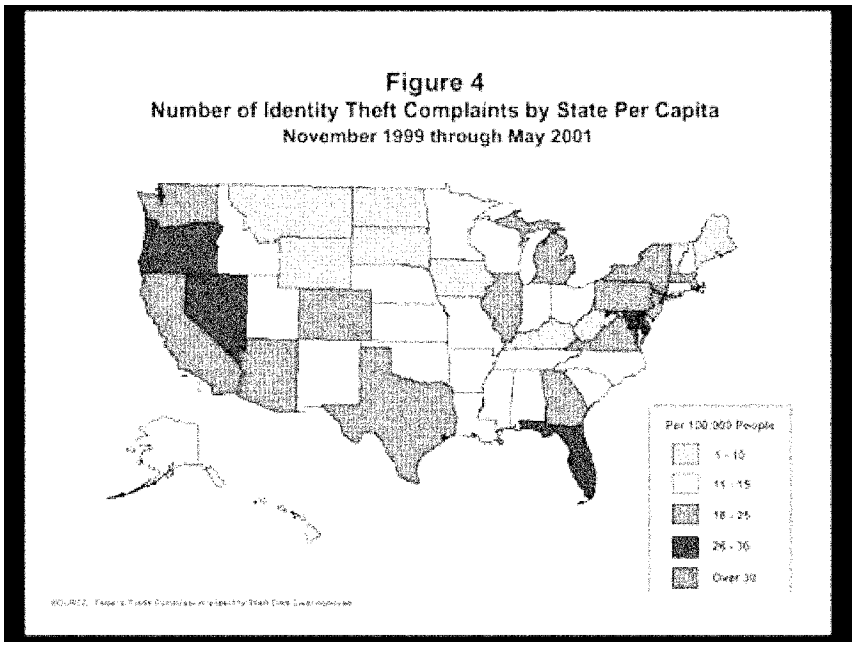


Figure 4
Number of Identity Theft Complaints by State Per Capita
November 1999 through May 2001
Per 100,000 People
1 - 10
11 - 15
16 - 25
26 - 30
Over 30

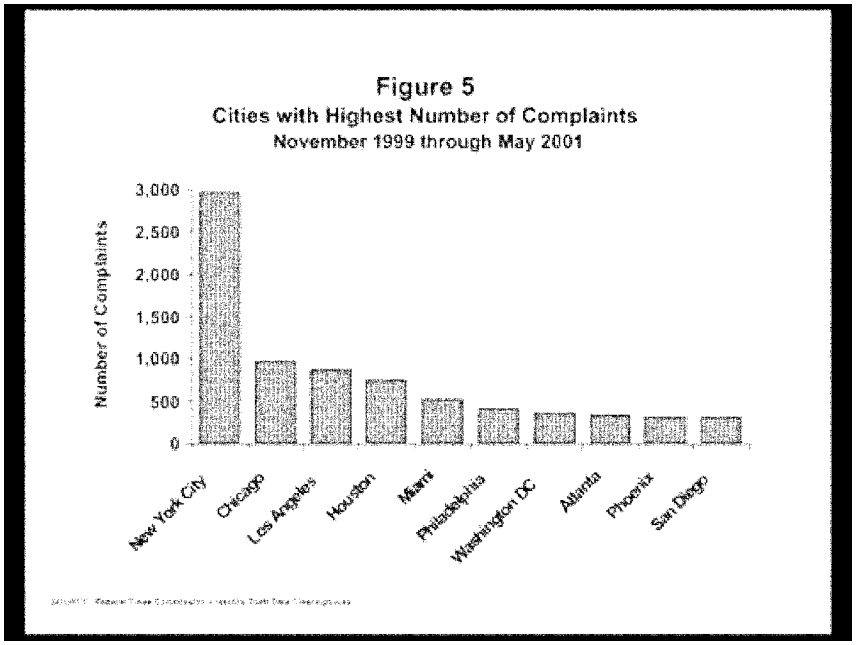


Figure 5
Cities with Highest Number of Complaints
November 1999 through May 2001
Number of Complaints
3,000
2,500
2,000
1,500
1,000
500
0
New York City
Chicago
Los Angeles
Houston
Miami
Philadelphia
Washington DC
Atlanta
Phoenix
San Diego

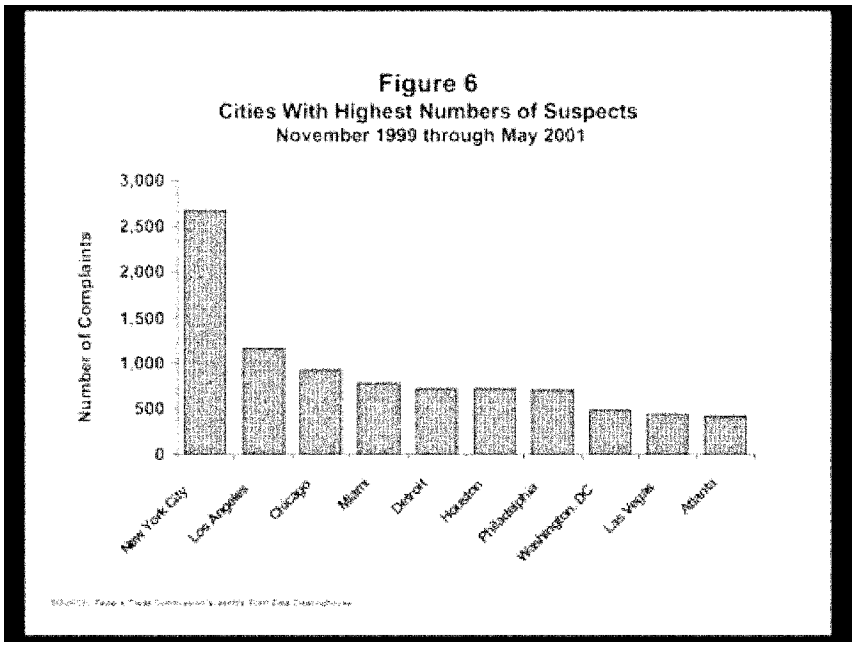
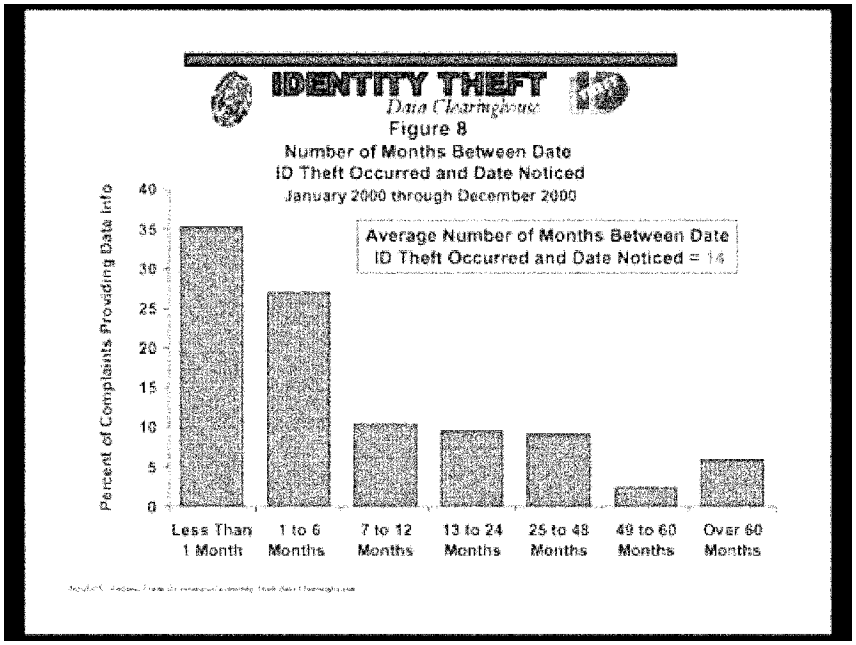


Figure 6
Cities With Highest Numbers of Suspects
November 1999 through May 2001
Number of Complaints
3,000
2,500
2,000
1,500
1,000
500
0
New York City
Los Angeles
Chicago
Miami
Detroit
Houston
Philadelphia
Washington, DC
Las Vegas
Atlanta


IDENTITY THEFT
Data Clearinghouse
Figure 8
Number of Months Between Date
ID Theft Occurred and Date Noticed
January 2000 through December 2000
Average Number of Months Between Date
ID Theft Occurred and Date Noticed = 14
Percent of Complaints Providing Date Info
40
35
30
25
20
15
10
5
0
Less Than 1 Month
1 to 6 Months
7 to 12 Months
13 to 24 Months
25 to 48 Months
49 to 60 Months
Over 60 Months

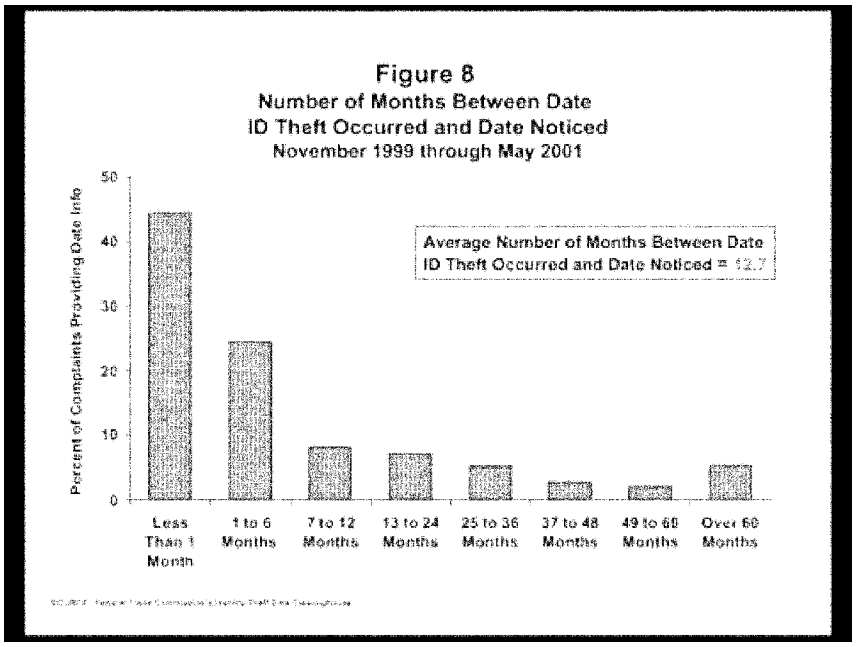


Figure 8
Number of Months Between Date
ID Theft Occurred and Date Noticed
November 1999 through May 2001
Average Number of Months Between Date
ID Theft Occurred and Date Noticed = 12.7
Percent of Complaints Providing Date Info
50
40
30
20
10
0
Less Than 1 Month
1 to 6 Months
7 to 12 Months
13 to 24 Months
25 to 36 Months
37 to 48 Months
49 to 60 Months
Over 60 Months

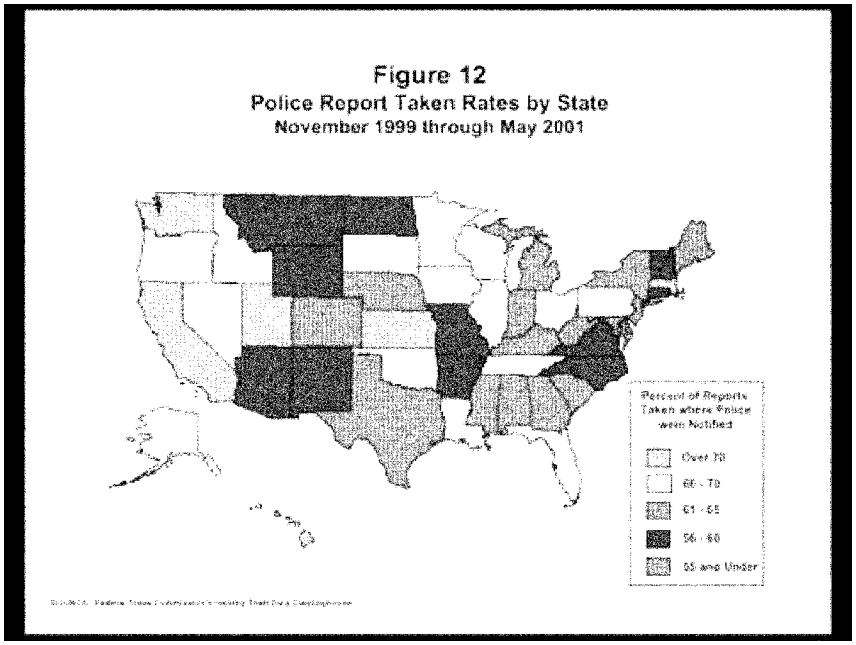
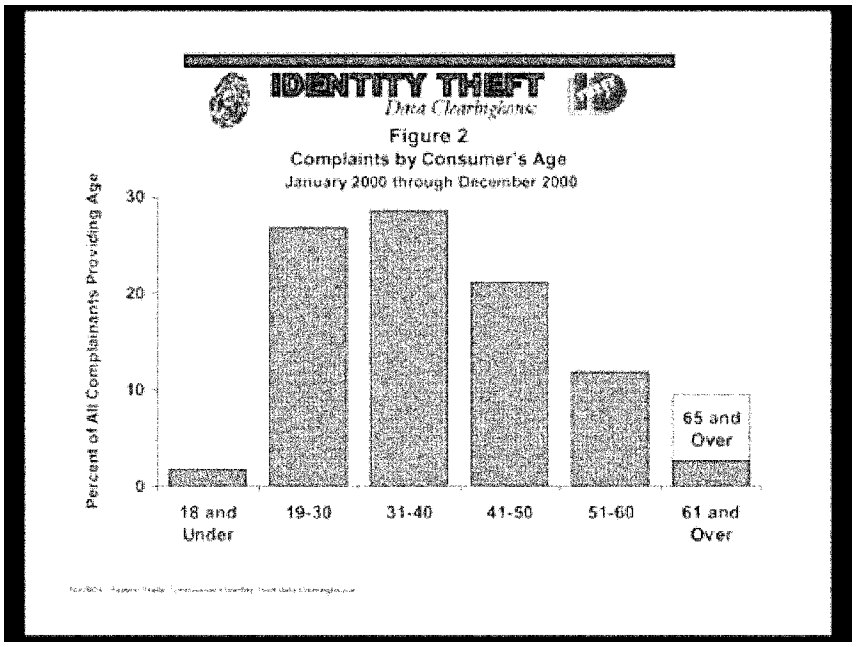
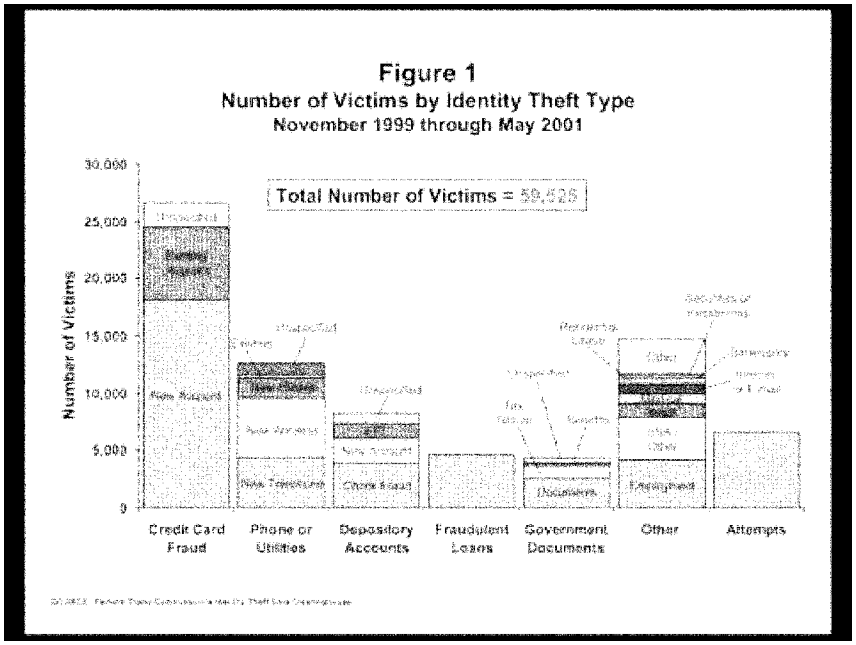


Figure 12
Police Report Taken Rates by State
November 1999 through May 2001
Percent of Reports Taken where Police were Notified
Over 70
66 - 70
61 - 65
56 - 60
55 and Under


IDENTITY THEFT
Data Clearinghouse
Figure 2
Complaints by Consumer's Age
January 2000 through December 2000
Percent of All Complainants Providing Age
30
20
10
0
18 and Under
19-30
31-40
41-50
51-60
61 and Over
65 and Over



Prosecution of ID Fraud

- General confusion on the part of law enforcement as to the crime and authority to investigate
- Law enforcement difficulties in tracking the extent of id fraud - identifying the extent of the defendant's criminal conduct

Prosecution Obstacles Case Reporting

- Lack of general public awareness
  - lack of attention to credit reports and other indices that would indicate to the victim that they have been victimized
  - Causes large time lapse between occurrence of the crime and its report
  - time delay causes leads to be cold and evidence to be difficult to obtain
  - possible statute of limitations problems
    - 3 year sol or within a year of discovery but no more than 6 years in addition

---

Prosecution Obstacles Case Generation

- Lack of Awareness on part of law enforcement and prosecutors as to Florida's Identity Fraud Statute
  - reporting consumer victim is not always perceived as a victim by law enforcement since the consumer is not generally the one bearing the financial loss, the financial institution bears the loss
  - institutional victims were historically more resistant to reporting the fraud

Prosecution Obstacle Jurisdiction and Venue

- Where did the crime occur?
  - Florida consumer denied credit because criminal in California committed identity fraud and ran up $10,000 in credit card bills.
    - Where did the crime occur?
    - Who can prosecute?
    - Where does venue lie?
    - Will California prosecute this case?

Restitution / Damages

- Identity Fraud Costs are Difficult to Determine
  - No comprehensive or agreed-upon way to estimate economic costs
  - costs could be high if identity fraud is an element of many financial crimes
  - human costs can be substantial
    - victim may be unable to obtain a job, purchase a car, or qualify for a mortgage – their life is essentially "on-hold" until their credit reports are restored
  - could take years to identify all of the effects

Sentencing Issues

- Identity Fraud Statute is a third degree felony.
  - Difficult to get an incarcerative sentence
  - limited to 5 years probation to pay restitution
  - Statute addresses restitution issues related to the victim having to devote time and resources to "cleaning up the mess" but needs to be more streamlined.

How do we overcome the hurdles?

- Provide for an education campaign to alert consumers to the realities of identity fraud, precautions that can be taken to minimize risk and what steps to take if they discover they have been victimized.
- Provide education for law enforcement and prosecutors on the issues presented in an identity fraud investigation.

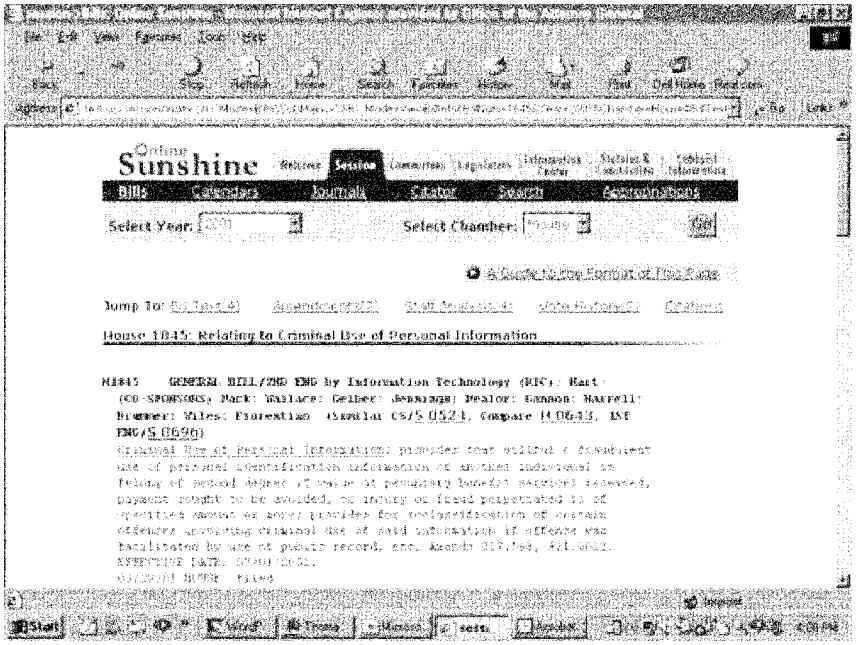
Clearing the Hurdles

- Statutory modifications to the statute to make it clear that venue lies in the victim's county of residence.
- Statutory modifications to the felony classification statute identifying identity fraud as a level 4 felony
- Statutory modifications enhancing the penalties if public records are used to facilitate or further the identity fraud

---

Clearing the Hurdles

- Statutory modifications that make it easier for the prosecutor to secure restitution for all victims even if they are not named in the charging document. Aggravated white collar crime bill.



Other Areas of Concern

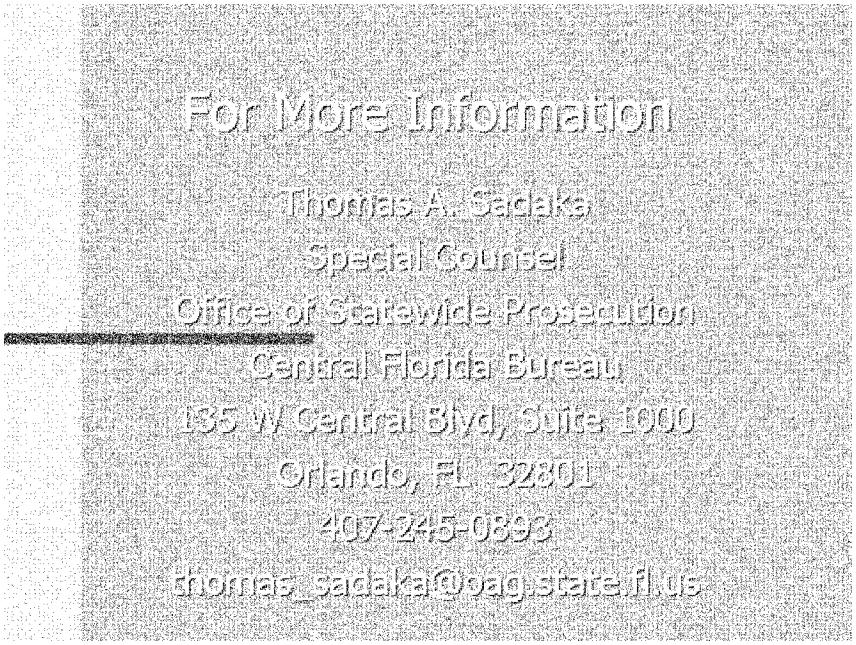
- Abuse of Chapter 119 by persons with fraudulent intent.
  - Identity fraud committed utilizing a Financial Affidavit filed in a dissolution of marriage case.
  - Insurance Fraud committed by securing an automobile accident report
- 817 will now enhance the sentence of an individual who has used Chapt. 119 information for criminal purposes.

Other Areas of Concern

- The "Not Me" Division
  - Use of SAO resources in "protecting the innocent"
  - Investigators or support personnel who secure finger prints and other information from the "not me"
- Obligation of Worthless Check Divisions to minimize prosecution of a victim?

Other Areas of Concern

- Cleaning up the mess of ID Fraud
  - Removing Warrants issued against the victim
  - Removing arrests and prosecutions that have been levied against the victim
- Keeping ourselves from being victims of ID Fraud
  - don't freely give out personal information
  - don't leave financial and personal information laying about
  - shred everything...



Chairman SHAW. Thank you. Ms. Bovbjerg?

STATEMENT OF BARBARA D. BOVBJERG, DIRECTOR, EDUCATION, WORKFORCE, AND INCOME SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY KAY BROWN, ASSISTANT DIRECTOR

Ms. BOVBJERG. Thank you. Mr. Chairman, Mr. Foley, thank you very much for inviting me once again before the Subcommittee, and I am especially appreciative that you have chosen to meet in the beautiful Sunshine State. It is very nice to get away from Washington.

You have heard people talking about identity theft and the role of the Social Security Number in particular. And you have invited me today to discuss specifically government uses and protections of Social Security Numbers and the results of our ongoing work. I would like to focus first on uses and protections in the course of providing government benefits and services and then, second, on uses and protections in public records.

My testimony is based on surveys and site visits we conducted at Federal, State, and county government agencies in the past year. We are conducting this work at your request, Mr. Chairman, and we plan to issue our report next month.

Let me speak first about government uses in benefit and service provision. Federal, State and county agencies rely extensively on the Social Security Number, because SSNs provide a quick and efficient means of managing records and maintaining program integ-

rity. The numbers are particularly useful when agencies share information with others to verify benefit eligibility or to collect outstanding debt. Most of this data sharing occurs between government agencies, but a significant percentage of agencies we surveyed told us they also share with other entities, such as contractors, credit bureaus, and insurance companies. governments also use SSNs in their role as employers for wage reporting and benefit administration.

Although government agencies told us of various steps they take to safeguard the SSNs they use for these purposes, we found that certain key protections are not uniformly in place at any level of government. For example, when requesting SSNs, government agencies told us that they are not consistently providing individuals with key information mandated by Federal law. The Privacy Act requires that any Federal, State or local government agencies tell individuals who are asked to provide their SSNs whether the compliance is voluntary or mandatory and how the SSN will be used. This notification helps an individual make an informed decision and represents the first line of defense against improper use.

We also found that many government agencies occasionally display SSNs on documents that may be viewed by others who don't need this information. These documents include things like payroll and benefit checks, child care vouchers and official letters to program participants. In addition, some governments display employees' SSNs on employee badges and identification cards.

Responses to our surveys also showed potential weaknesses in information security. We asked agencies about eight practices commonly used in information security programs. Although many government agencies reported adopting some of the practices, none of the eight practices were uniformly adopted at any level of government.

Let me turn now to the topic of SSNs in public records. When I say public records, I mean records or documents routinely made available to the public for inspection, such as marriage licenses or property transactions. Some Federal agencies and many of the State and county agencies we surveyed, including courts at all three levels of government, told us they maintain public records that contain SSNs. Officials who maintain these records told us it is their responsibility to preserve the integrity of the record and to make it publicly available rather than to protect the privacy of the individual SSN holder. Nonetheless, we found examples of government entities trying innovative approaches to protect the SSNs in such records, including developing new forms that shield SSNs from public view by maintaining them separately or on the back of the rest of the record. These changes are most effective when the government agency prepares the documents itself, but they don't protect information on documents prepared and submitted by someone else nor do they limit the availability of SSNs on records filed prior to the change in form.

As a practical matter, as long as access to public records remains an in-person process, access will be somewhat limited. Where those wishing to view public records must visit a physical location and request information on a case-by-case basis, there is a measure of protection against widespread collection of personal information,

like the SSN. However, several officials told us that thanks to the growth of electronic recordkeeping, they were considering making such records available on their Web sites. Such actions would create new opportunities for gathering SSNs from public records on a broad scale.

In conclusion, governments use SSNs for many beneficial purposes but they do not always ensure that this personal information is protected. Although it is unclear whether these gaps in protection lead directly to identity theft, they represent a potential for SSN misuse. It will be important for governments at all levels to consider how best to protect SSNs and to take appropriate actions to improve the security of this information. Thank you, Mr. Chairman.

[The prepared statement of Ms. Bovbjerg follows:]

Statement of Barara D. Bovbjerg, Director, Education, Workforce, and Income Security Issues, U.S. General Accounting Office

Chairman Shaw and members of the Subcommittee:

Thank you for inviting me here today to discuss government use of Social Security Numbers (SSNs). Although the SSN was originally created in 1936 as a means to track workers' earnings and eligibility for Social Security benefits, today the number is used for myriad non-Social Security purposes in both the private and public sectors. Consequently, the public is concerned with how their personal SSNs are being used and protected. Further, the growth in electronic record keeping and the explosion of the availability of information over the Internet, combined with the rise in reports of identity theft, have heightened this concern.

We have previously reported that SSNs play an important role in public and private sectors' ability to deliver services or conduct business.[1] Today, I will focus on how federal, state, and local governments use SSNs. Specifically, I will discuss (1) the extent and nature of government agencies' use of SSNs as they administer programs to provide benefits and services and the actions government agencies take to safeguard these SSNs from improper disclosure and (2) the extent and nature of governments' use of SSNs when they are contained in public records and the options available to better safeguard SSNs that are traditionally found in these public records.[2] My testimony is based on our ongoing work conducted at your request and that of the Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary. To address these issues, we mailed surveys to programs in 18 federal agencies and those departments that typically use SSNs in all 50 states, the District of Columbia, and the 90 most populous counties.[3] We also conducted site visits and in-depth interviews at six selected federal programs, three states, and three counties. We met with officials responsible for programs, agencies, or departments (hereinafter referred to generically as agencies) and courts that make frequent use of SSNs. We conducted our work between February 2001 and March 2002 in accordance with generally accepted government auditing standards.

In summary, in delivering services and benefits to the public, federal, state, and county government agencies use SSNs to manage records, verify the eligibility of benefit applicants, collect outstanding debts and conduct research and program evaluation. Using SSNs for these purposes can save the government and taxpayers hundreds of millions of dollars each year. As they make use of SSNs for these purposes, government agencies are taking some steps to safeguard the numbers. However, agencies are not consistently following federal laws regarding the collection of per-

[1] U.S. General Accounting Office, Social Security: Government and Commercial Use of the Social Security Number is Widespread, GAO/HEHS–99–28 (Washington, D.C.: Feb. 16, 1999).

[2] We found no commonly accepted definition of public records. For the purposes of this statement, when we use the term public record, we are referring to a record or document that is routinely made available to the public for inspection either by a federal, state, or local government agency or a court, such as those readily available at a public reading room, clerk's office, or on the Internet.

[3] We did not survey state Departments of Motor Vehicles or state agencies that administer state tax programs, because we have reported on these activities separately. See U.S. General Accounting Office, Child Support Enforcement: Most States Collect Drivers' SSNs and Use Them to Enforce Child Support, GAO–02–239 (Washington, D.C.: Feb. 15, 2002) and Taxpayer Confidentiality: Federal, State, and Local Agencies Receiving Taxpayer Information, GAO–GGD–99–164 (Washington, D.C.: Aug. 30, 1999).

sonal information, implementing safeguards to protect SSNs from improper disclosure, or limiting the display of SSN on documents not intended for the public. Moreover, courts at all three levels of government and certain offices at the state and county level maintain records that contain SSNs for the purpose of making them available to the public. Recognizing that these SSNs may be misused by others, some government entities have taken steps to protect the SSNs from public display. For example, some have modified forms so that they can collect SSNs but keep them in a file separate from the public portion of the record. Nonetheless, although public records have traditionally been housed in government offices and court buildings, to improve customer service some government entities are considering placing more public records on the Internet. The ease of access the Internet affords could encourage individuals to engage in information gathering from public records on a broader scale than possible previously. In conclusion, we will be reporting in more detail on these issues at the end of this month and look forward to exploring additional options to better protect SSNs with you as we complete our work.

Background

The use of SSNs by government and the private sector has grown over time, in part because of federal requirements. In addition, the growth in computerized records has further increased reliance on SSNs. This growth in use and availability of the SSN is important because SSNs are often one of the "identifiers" of choice among identity thieves. Although no single federal law regulates the use and disclosure of SSNs by governments, when federal government agencies use them, several federal laws limit the use and disclosure of the number.[4] Also, state laws may impose restrictions on SSN use and disclosure, and they vary from state to state. Moreover, some records that contain SSNs are considered part of the public record and, as such, are routinely made available to the public for review.

SSN Use Has Grown, in Part Because of Federal Requirements

Since the creation of the SSN, the number of federal agencies and others that rely on it has grown beyond the original intended purpose. In 1936, the Social Security Administration (SSA) created a numbering system designed to provide a unique identifier, the SSN, to each individual. The agency uses SSNs to track workers' earnings and eligibility for Social Security benefits, and as of December 1998, SSA had issued 391 million SSNs. Since the creation of the SSN, other entities in both the public and private sectors have begun using SSNs, in part because of federal requirements. The number of federal agencies and others relying on the SSN as a primary identifier escalated dramatically, in part, because a number of federal laws were passed that authorized or required its use for specific activities. (See appendix I for examples of federal laws that authorize or mandate the collection and use of SSNs.) In addition, private businesses, such as financial institutions and health care service providers, also rely on individuals SSNs. In some cases, they require the SSN to comply with federal laws but, at other times, they routinely choose to use the SSNs to conduct business.

In addition, the advent of computerized records further increased reliance on SSNs. Government entities are beginning to make their records electronically available over the Internet. Moreover, the Government Paperwork Elimination Act of 1998 requires that, where practicable, federal agencies provide by 2003 for the option of the electronic maintenance, submission, or disclosure of information. State government agencies have also initiated Web sites to address electronic government initiatives. Moreover, continuing advances in computer technology and the ready availability of computerized data have spurred the growth of new business activities that involve the compilation of vast amounts of personal information about members of the public, including SSNs, that businesses sell.

Identity Thieves Often Use SSNs

The overall growth in the use of SSNs is important to individual SSN holders because these numbers, along with names and birth certificates, are among the three personal identifiers most often sought by identity thieves.[5] Identity theft is a crime that can affect all Americans. It occurs when an individual steals another individual's personal identifying information and uses it fraudulently. For example, SSNs and other personal information are used to fraudulently obtain credit cards, open utility accounts, access existing financial accounts, commit bank fraud, file false tax returns, and falsely obtain employment and government benefits. SSNs play an im-

[4] In this review, we do not include criminal provisions that might apply to the improper use of SSNs.

[5] United States Sentencing Commission, Identity Theft Final Alert (Washington, D.C.: Dec. 15, 1999).

portant role in identity theft because they are used as breeder information to create additional false identification documents, such as drivers licenses.

Recent statistics collected by federal and consumer reporting agencies indicate that the incidence of identity theft appears to be growing.[6] The Federal Trade Commission (FTC), the agency responsible for tracking identity theft, reports that complaint calls from possible victims of identity theft grew from about 445 calls per week in November 1999, when it began collecting this information, to about 3,000 calls per week by December 2001. However, FTC noted that this increase in calls might also, in part, reflect enhanced consumer awareness. In addition, SSA's Office of the Inspector General, which operates a fraud hotline, reports that allegations of SSN misuse increased from about 11,000 in fiscal year 1998 to more than 65,200 in fiscal year 2001. However, some of the reported increase may be a result of a growth in the number of staff SSA assigned to field calls to the Fraud Hotline during this period. SSA staff increased from 11 to over 50 during this period, which allowed personnel to answer more calls. Also, officials from two of the three national consumer reporting agencies report an increase in the number of 7 year fraud alerts placed on consumer credit files, which they consider to be reliable indicators of the incidence of identity theft.[7] Finally, it is difficult to determine how many individuals are prosecuted for identity theft because law enforcement entities report that identity theft is almost always a component of other crimes, such as bank fraud or credit card fraud, and may be prosecuted under the statutes covering those crimes.

Most often, identity thieves use SSNs belonging to real people rather than making one up; however, on the basis of a review of identify theft reports, victims usually (75 percent of the time) did not know where or how the thieves got their personal information.[8] In the 25 percent of the time when the source was known, the personal information, including SSNs, usually was obtained illegally. In these cases, identity thieves most often gained access to this personal information by taking advantage of an existing relationship with the victim. The next most common means of gaining access were by stealing information from purses, wallets, or the mail. In addition, individuals can also obtain SSNs from their workplace and use them themselves or sell them to others. Finally, SSNs and other identifying information can be obtained legally through Internet sites maintained by both the public and private sectors and from records routinely made available to the public by government entities and courts. Because the sources of identity theft cannot be more accurately pinpointed, it is not possible at this time to determine the extent to which the government's use of SSNs contributes to this problem as compared to use of SSNs by the private sector.

In Some Instances, SSNs Are to Be Protected from Public Disclosure

No single federal law regulates the overall use or restricts the disclosure of SSNs by governments; however, a number of laws limit SSN use in specific circumstances. Generally, the federal government's overall use and disclosure of SSNs are restricted under the Freedom of Information Act and the Privacy Act. The Freedom of Information Act presumes federal government records are available upon formal request, but exempts certain personal information, such as SSNs. The purpose of the Privacy Act, broadly speaking, is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy by federal agencies. Also, the Social Security Act Amendments of 1990 provide some limits on disclosure, and these limits apply to state and local governments as well. In addition, a number of federal statutes impose certain restrictions on SSN use and disclosure for specific programs or activities.[9] At the state and county level, each state may have its own statutes ad-

[6] U.S. General Accounting Office, Identity Theft: Prevalence and Cost Appear to be Growing, GAO–02–363 (Washington, D.C.: Mar. 1, 2002).

[7] A fraud alert is a warning that someone may be using the consumer's personal information to fraudulently obtain credit. When a fraud alert is placed on a consumer's credit card file, it advises credit grantors to conduct additional identity verification before granting credit. The third consumer reporting office offers fraud alerts that can vary from 2 to 7 years at the discretion of the individual.

[8] This information is based on a review of 39 cases involving SSN theft drawn from the Federal Trade Commission's fiscal year 1998 datafiles.

[9] For example, the Internal Revenue Code, which requires the use of SSNs for certain purposes, declares tax return information, including SSNs, to be confidential, limits access to specific organizations, and prescribes both civil and criminal penalties for unauthorized disclosure. For more information, see GAO–GGD–99–164. Also, the Personal Responsibility and Work Opportunity Act of 1996 explicitly restricts the use of SSNs to purposes set out in the Act, such as locating absentee parents to collect child support payments.

dressing the public's access to government records and privacy matters; therefore, states may vary in terms of the restrictions they impose on SSN use and disclosure.

In addition, a number of laws provide protection for sensitive information, such as SSNs, when maintained in computer systems and other government records. Most recently, the Government Information Security Reform provisions of the Fiscal Year 2001 Defense Authorization Act require that federal agencies take specific measures to safeguard computer systems that may contain SSNs.[10] For example, federal agencies must develop an agency-wide information security management program. These laws do not apply to state and local governments; however, in some cases state and local governments have developed their own statutes or put requirements in place to similarly safeguard sensitive information, including SSNs, kept in their computer systems.

SSNs Are Found in Some Public Records

In addition to the SSNs used by program agencies to provide benefits or services, some records that contain SSNs are considered part of the public record and, as such, are routinely made available to the public for review. This is particularly true at the state and county level. Generally, state law governs whether and under what circumstances these records are made available to the public, and they vary from state to state. They may be made available for a number of reasons. These include the presumption that citizens need government information to assist in oversight and ensure that government is accountable to the people. Certain records maintained by federal, state, and county courts are also routinely made available to the public. In principle, these records are open to aid in preserving the integrity of the judicial process and to enhance the public trust and confidence in the judicial process. At the federal level, access to court documents generally has its grounding in common law and constitutional principles. In some cases, public access is also required by statute, as is the case for papers filed in a bankruptcy proceeding. As with federal courts, requirements regarding access to state and local court records may have a state common law or constitutional basis or may be based on state laws.

SSNs Are Widely Used by Program Agencies at All Levels of Government, but Could Be Better Protected by Them

When federal, state, and county government agencies administer programs that deliver services and benefits to the public, they rely extensively on the SSNs of those receiving the benefits and services. SSNs provide a quick and efficient means of managing records and are used to conduct research and program evaluation. In addition, they are particularly useful when agencies share information with others to verify the eligibility of benefit applicants or to collect outstanding debts. Using SSNs for these purposes can save the government and taxpayers hundreds of millions of dollars each year. As they make this wide use of SSNs, government agencies are taking some steps to safeguard the numbers; however, certain key measures that could help protect SSNs are not uniformly in place at any level of government. First, when requesting SSNs, government agencies are not consistently providing individuals with key information mandated by federal law, such as whether individuals are required to provide their SSNs. Second, although agencies that use SSNs to provide benefits and services are taking steps to safeguard them from improper disclosure, our survey identified potential weaknesses in the security of information systems at all levels of government. Similarly, sometimes government agencies display SSNs on documents not intended for the public, and we found numerous examples of actions taken to limit the presence of SSNs on documents. However, these changes are not systematic and many government agencies continue to display SSNs on a variety of documents.

All Levels of Government Use SSNs Extensively for a Wide Range of Purposes

Most of the agencies we surveyed at all levels of government reported using SSNs extensively to administer their programs.[11] As shown in table 1, more agencies reported using SSNs for internal administrative purposes, such as using SSNs to identify, retrieve, and update their records, than for any other purpose. SSNs are so widely used for this purpose, in part, because each number is unique to an indi-

[10] These provisions supplement information security requirements established in the federal Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and Office of Management and Budget guidance.

[11] Of the respondents to our survey, 14 state program departments and 13 county program departments reported that they do not obtain, receive, or use the SSN of program participants, service recipients, or individual members of the public. We did not verify this information.

vidual and does not change, unlike some other personal identifying information, such as names and addresses.

Table 1: Percentage of Program Agencies Using SSNs for Each Reason Listed

Purpose of SSN Use	Federal (N=55)[a] Percent	State (N=244) Percent	County (N=197) Percent
Internal administrative purposes	82	90	89
Sharing			
Verify applicants' eligibility; monitor accuracy of information individuals provide	73	83	82
Collect debts individuals owe agency/government	40	34	25
Research and Evaluation			
Conduct internal research or program evaluation	53	44	26
Provide data to outside researchers	4	18	7

[a] Total number of possible respondents

Source: GAO surveys of federal, state, and county departments and agencies. Table includes departments and agencies that administer programs and excludes courts, county clerks and recorders, and state licensing agencies. It excludes state departments of motor vehicles and tax administration.

Many agencies also use SSNs to share information with other entities to bolster the integrity of the programs they administer. For example, the majority of agencies at all three levels of government reported sharing information containing SSNs for the purpose of verifying an applicant's eligibility for services or benefits. Agencies use applicants' SSNs to match the information they provide with information in other data bases, such as other federal benefit paying agencies, state unemployment agencies, the Internal Revenue Service, or employers. As unique identifiers, SSNs help ensure that the agency is matching information on the correct person. Also, some agencies at each level of government reported sharing data containing SSNs to collect debts owed them. Using SSNs for these purposes can save the government and taxpayers hundreds of millions of dollars, such as when SSA matched its data on Supplemental Security Income recipients with state and local correctional facilities to identify prisoners who were no longer eligible for benefits.[12] Doing so helped identify more than $150 million in Supplemental Security Income overpayments and prevented improper payments of more than $170 million over an 8-month period. Finally, SSNs along with other program data, are sometimes used for statistical programs, research, and evaluation, in part because they provide government agencies and others with an effective mechanism for linking data on program participation with data from other sources.[13]

When government agencies that administer programs share records containing individuals' SSNs with other entities, they are most likely to share them with other government agencies.[14] After that, the largest percentage of federal and state program agencies report sharing SSNs with contractors (54 and 39 percent respectively), and a relatively large percentage of county program agencies report sharing with contractors as well (28 percent). Agencies across all levels of government use contractors to help them fulfill their program responsibilities, such as determining eligibility for services and conducting data processing activities. In addition to sharing SSNs with contractors, government agencies also share SSNs with private busi-

[12] SSI provides cash assistance to needy individuals who are aged, blind, or disabled.

[13] In some cases, records containing SSNs are sometimes matched across multiple agency or program databases. The statistical and research communities refer to the process of matching records containing SSNs for statistical or research purposes as "record linkage." See U.S. General Accounting Office, Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information, GAO–01–126SP (Washington, D.C.: Apr. 2001).

[14] On the federal level, data sharing often involves computerized record matching. The Computer Matching and Privacy Protection Act of 1988, which amended the Privacy Act, specifies procedural safeguards affecting agencies' use of Privacy Act records in performing certain types of computerized matching programs, including due process rights for individuals whose records are being matched. These due process rights were further clarified in the Computer Matching and Privacy Protection Amendments of 1990.

nesses, such as credit bureaus and insurance companies, as well as debt collection agencies, researchers, and, to a lesser extent, with private investigators.

In addition, all government personnel departments we surveyed reported using their employees' SSNs to fulfill at least some of their responsibilities as employers. Aside from requiring that employers report on their employees' wages to SSA, federal law also requires that states maintain employers' reports of newly hired employees identified by SSN. The national database is used by state child support agencies to locate parents who are delinquent in child support payments. In addition, employers responding to our survey said they use SSNs to help them maintain internal records and provide employee benefits. To provide these benefits, employers often share data on employees with other entities, such as health care providers or pension plan administrators.

Many Government Entities Collect SSNs without Providing Required Information

When a government agency requests an individual's SSN, the individual needs certain information to make an informed decision about whether to provide their SSN to the government agency or not. Accordingly, section 7 of the Privacy Act requires that any federal, state, or local government agency, when requesting an SSN from an individual, provide that individual with three key pieces of information.[15] Government entities must

- tell individuals whether disclosing their SSNs is mandatory or voluntary;
- cite the statutory or other authority under which the request is being made; and
- state what uses government will make of the individual's SSN.

This information, which helps the individual make an informed decision, is the first line of defense against improper use.

Although nearly all government entities we surveyed collect and use SSNs for a variety of reasons, many of these entities reported they do not provide individuals the information required under section 7 of the Privacy Act when requesting their SSNs. Federal agencies were more likely to report that they provided the required information to individuals when requesting their SSNs than were states or local government agencies. Even so, federal agencies did not consistently provide this required information; 32 percent did not inform individuals of the statutory authority for requesting the SSN and 21 percent of federal agencies reported that they did not inform individuals of how their SSNs would be used. At the state level, about half of the respondents reported providing individuals with the required information, and at the county level, about 40 percent of the respondents reported doing so.

Many Agencies Using SSNs to Administer Programs Do Not Have Uniform Information Security Controls in Place

When government agencies collect and use SSNs as an essential component of their operations, they need to take steps to mitigate the risk of individuals gaining unauthorized access to SSNs or making improper disclosure or use of SSNs. Over 90 percent of our survey respondents reported using both hard copy and electronic records containing SSNs when conducting their program activities. When using electronic media, many employ personal computers linked to computer networks to store and process the information they collect. This extensive use of SSNs, as well as the various ways in which SSNs are stored and accessed or shared, increase the risks to individuals' privacy and make it both important and challenging for agencies to take steps to safeguard these SSNs.

No uniform guidelines specify what actions governments should take to safeguard personal information that includes SSNs. However, to gain a better understanding of whether agencies had measures in place to safeguard SSNs, we selected eight commonly used practices found in information security programs, and we surveyed the federal, state, and county programs and agencies on their use of these eight practices. Responses to our survey indicate that agencies that administer programs at all levels of government are taking some steps to safeguard SSNs; however, potential weaknesses exist at all levels. Many survey respondents reported adopting some of the practices; however, none of the eight practices were uniformly adopted at any level of government. In general, when compared to state and county government agencies, a higher percentage of federal agencies reported using most of the eight practices. However, despite the federal government's self-reported more frequent use of these practices relative to the state and counties, it is important to note that since 1996 we have consistently identified significant information security

[15] Section 7 of the Privacy Act is not codified with the rest of the act, but rather is found in the note section to 5 U.S.C. 552a.

weaknesses across the federal government. We are not aware of a comparable comprehensive assessments of information security for either state or county government. (For additional information on the eight practices we selected and how they fit into the federal framework for an information security program, see appendix II.)

Further, when SSNs are passed from a government agency to another entity, agencies need to take additional steps to continue protections for sensitive personal information that includes SSNs, such as imposing restrictions on the entities to help ensure that the SSNs are safeguarded.[16] Responses to our survey indicate that, when sharing such sensitive information, most agencies reported requiring those receiving personal data to restrict access to and disclosure of records containing SSNs to authorized persons and to keep records in secured locations. However, fewer agencies reported having provisions in place to oversee or enforce compliance with these requirements.

Government Agencies Display SSNs on Documents Not Intended for the Public

In the course of delivering their services or benefits, many government agencies occasionally display SSNs on documents that may be viewed by others, some of whom may not have a need for this personal information. These documents include payroll checks, vouchers for tax credits for childcare, travel orders, and authorization for training outside of the agency. Also, some personnel departments reported displaying employees' SSNs on their employee badges (27 percent of federal respondents, 5 percent of state, and 9 percent of county). Notably, the Department of Defense (DOD), which has over 2.9 million military and civilian personnel, displays SSNs on its military and civilian identification cards. On the state level, the Department of Criminal Justice in one state, which has about 40,000 employees, displays SSNs on all employee identification cards. According to department officials, some of their employees have taken actions such as taping over their SSNs so that prison inmates and others cannot view this personal information.

SSNs are also displayed on documents that are not employee-related. For example, some benefit programs display the SSN on the benefit checks and eligibility cards, and over one-third of federal respondents reported including the SSN on official letters mailed to participants. Further, some state institutions of higher education display students' SSNs on identification cards. Finally, SSNs are sometimes displayed on business permits that must be posted in public view at an individual's place of business.

In addition to these examples of SSN display, we also identified a number of instances where the Congress or governmental entities have taken or are considering action to reduce the presence of SSNs on documents that may be viewed by others. For example, the DOD commissary stopped requiring SSNs on checks written by members because of concerns about improper use of the SSNs and identity theft.[17] Also, a state comptroller's office changed its procedures so that it now offers vendors the option of not displaying SSNs on their business permits. Finally, some states have passed laws prohibiting the use of SSNs as a student identification number.

These efforts to reduce display suggest a growing awareness that SSNs are private information, and the risk to the individual of placing an SSN on a document that others can see may be greater than the benefit to the agency of using the SSN in this manner. However, despite this growing awareness and the actions cited above, many government agencies continue to display SSNs on a variety of documents that can be seen by others.

Open Nature of Certain Government Records Results in Wide Access to SSNs but Alternatives Exist

Regarding public records, many of the state and county agencies responding to our survey reported maintaining records that contain SSNs; however federal program agencies maintain public records less frequently. At the state and county levels, certain offices, such as state licensing agencies and county recorders' offices, have traditionally been repositories for public records that may contain SSNs. In addition, courts at all three levels of government maintain public records that may contain SSNs. Officials who maintain these records told us their responsibility is to preserve the integrity of the record rather than protect the privacy of the individual SSN holder. However, we found examples of some government entities that are trying innovative approaches to protect the SSNs in such records from public display.

[16] In some cases, where federal agencies administer programs that provide federal funds to states and counties, the federal agency has spelled out program-specific requirements for information security that state and county government agencies are expected to follow when they use federal funds to operate these programs.

[17] As of March 2002, the Navy Commissary still requires SSNs on checks. Officials told us they hope to implement a system similar to the DOD Commissary by the end of 2002.

Moreover, the general public has traditionally gained access to public records by visiting the office that maintains the records, an inconvenience that represents a practical limitation on the volume of SSNs any one person can collect. However, the growth of electronic record-keeping places new pressures on agencies to provide their data to the pubic on the Internet. Although few entities report currently making public records containing SSNs available on the Internet, several officials told us they are considering expanding the volume and type of such records available on their Web site. This would create new opportunities for gathering SSNs on a broader scale. Again, some entities are considering alternatives to making SSNs available on such a wide scale, while others are not.

Many State and County Public Records Contain SSNs

As shown in table 2, more than two-thirds of the courts, county recorders, and state licensing agencies that reported maintaining public records reported that these records contained SSNs.[18] In addition, some program agencies also reported maintaining public records that contain SSNs.

Table 2: Of Courts, County Recorders, and State Licensing Agencies, and of Program Agencies That Maintain Public Records, Percentage That Maintain Public Records That Contain SSNs

	Federal		State		County	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Courts, recorders, and licensing agencies that maintain public records with SSNs	3/3	100	21/31	68	73/95	77
Program agencies that maintain public records with SSNs	4/22	23	54/189	29	46/140	33

Source: Data from GAO survey of federal, state, and county departments and agencies. It excludes state departments of motor vehicles and tax administration.

County clerks or recorders (hereinafter referred to as recorders) and certain state agencies often maintain records that contain SSNs because these offices have traditionally been the repository for key information that, among other things, chronicles various life events and other activities of individuals as they interact with government.[19] SSNs appear in these public records for a number of reasons. They may already be a part of a document that is submitted to a recorder for official preservation. For example, military veterans are encouraged to file their discharge papers, which contain SSNs, with their local recorder's office to establish a readily available record of their military service.[20] Also, documents that record financial transactions, such as tax liens and property settlements, contain SSNs to help identify the correct individual. In other cases, government officials are required by law to collect SSNs. For example, to aid in locating non-custodial parents who are delinquent in their child support payments, the federal Personal Responsibility and Work Opportunity Reconciliation Act of 1996 requires that states have laws in effect to collect SSNs on applications for marriage, professional, and occupational licenses. Moreover, some state laws allow government entities to collect SSNs on voter registries to help avoid duplicate registrations. Although the law requires public entities to collect the SSN as part of these activities, this does not necessarily mean that the SSNs always must be placed on the document that becomes part of the public record.

Courts at all three levels of government also collect and maintain records that are routinely made available to the public. Court records overall are presumed to be public; however, each court may have its own rules or practices governing the re-

[18] Of the respondents to our survey, 20 county recorders and courts and 5 state courts reported that they do not obtain, receive, or use the SSN of program participants, service recipients, or individual members of the public. We did not verify this information.

[19] It differs from state-to-state as to whether certain records, such as marriage licenses and birth certificates, are maintained in county or state offices. Certain documents, however, such as land and title transfers, are almost always maintained at the local, or county, level.

[20] Veterans are advised that these are important documents which can be registered/recorded in most states or localities for a nominal fee making retrieval easy. In October 2001, DOD added a cautionary statement that recording these documents could subject them to public access in some states or localities.

lease of information.[21] As with recorders, SSNs appear in court documents for a variety of reasons. In many cases, SSNs are already a part of documents that are submitted by attorneys or individuals. These documents could be submitted as part of the evidence for a proceeding or could be included in documents, such as a petition for an action, a judgment or a divorce decree. In other cases, courts include SSNs on documents they and other government officials create, such as criminal summonses, arrest warrants, and judgments, to increase the likelihood that the correct individual is affected (i.e. to avoid arresting the wrong John Smith). In some cases federal law requires that SSNs be placed in certain records that courts maintain, such as records pertaining to child support orders, divorce decrees, and paternity determinations. Again, this assists child support enforcement agencies in efforts to help parents collect money that is owed to them. These documents may also be maintained at county clerk or recorders' offices.

When federal, state, or county entities, including courts, maintain public records, they are generally prohibited from altering the formal documents. Officials told us that their primary and mandated interest is in preserving the integrity of the record rather than protecting the privacy of the individual named in the record. Officials told us they believe they have no choice but to accept the documents with the SSNs and fulfill the responsibility of their office by making them available to the general public.

Alternatives to Displaying SSNs in Public Records Exist

When creating public documents or records, such as marriage licenses, some government agencies are trying new innovative approaches that protect SSNs from public display. For example, some have developed alternative types of forms to keep SSNs and other personal information separate from the portion of a document that is accessible to the general public.[22] Changing how the information is captured on the form itself can help solve the dilemma of many county recorders who, because they are the official record keepers of the county, are usually not allowed to alter an original document after it is officially filed in their office. For example, a county recorder told us that Virginia recently changed its marriage license application so that the form is now in triplicate, and the copy that is available to the general public does not contain the SSN. However, an official told us even this seemingly simple change in the format of a document can be challenging because, in some cases, the forms used for certain transactions are prescribed by the state. In addition to these efforts at recorders offices, some courts have made efforts to protect SSNs in documents that the general public can access through court clerk offices. For example, one state court offers the option of filing a separate form containing the SSN that is kept separate from the part of the record that is available for public inspection.

These solutions, however, are most effective when the recorder's office, state agencies, and courts prepare the documents themselves. In those many instances where others file the documents, such as individuals, attorneys, or financial institutions, the receiving agency has less control over what is contained in the document and, in many cases, must accept it as submitted. Officials told us that, in these cases, educating the individuals who submit the documents for the record may help to reduce the appearance of SSNs. This would include individuals, financial institutions, title companies, and attorneys, who could begin by considering whether SSNs are required on the documents they submit. It may be possible to limit the display of SSNs on some of these documents or, where SSNs are deemed necessary to help identify the subject of the documents, it may be possible to truncate the SSN to the last four digits.

While the above options are available for public records created after an office institutes changes, fewer options exist to limit the availability of SSNs in records that have already been officially filed or created. One option is redacting or removing SSNs from documents before they are made available to the general public. In our fieldwork, we found instances where departments redact SSNs from copies of documents that are made available to the general public, but these tended to be situations where the volume of records and number of requests were minimal, such as in a small county. Most other officials told us redaction was not a practical alternative for public records their offices maintain. Although redaction would reduce the likelihood of SSNs being released to the general public, we were told it is time-con-

[21] In some states, for example, adoption records, grand jury records, and juvenile court records are not part of the public record. In addition, some court documents pertinent to the cases may or may not be in the public record, depending on local court practice. Finally, the judge can choose to explicitly seal a record to protect the information it contains from public review.

[22] In some cases, however, the law requires that the SSN appear on the document itself, as on death certificates.

suming, labor intensive, difficult, and in some cases would require change in law. In documents filed by others outside of the office, SSNs do not appear in a uniform place and could appear many times throughout a document. In these cases, it is a particularly lengthy and labor-intensive process to find and redact SSNs. Moreover, redaction would be less effective in those offices where members of the general public can inspect and copy large numbers of documents without supervision from office staff. In these situations, officials told us that they could change their procedures for documents that they collect in the future, but it would be extremely difficult and expensive to redact SSNs on documents that have already been collected and filed.

Traditional Access to Public Records Has Practical Limitations That Would Not Exist if the Records Were Placed on the Internet

Traditionally, the public has been able to gain access to SSNs contained in public records by visiting the recorder's office, state office, or court house; however, the requirement to visit a physical location and request or search for information on a case-by-case basis offers some measure of protection against the widespread collection and use of others' SSNs from public records.[23] Yet, this limited access to information in public records is not always the case. We found examples where members of the public can obtain easy access to larger volumes of documents containing SSNs. Some offices that maintain public records offer computer terminals on site where individuals can look up electronic files from a site-specific database. In one of the offices we visited, documents containing SSNs that were otherwise accessible to the public were also made available in bulk to certain groups. When asked about sharing information containing SSNs with other entities, a higher percentage of county recorders reported sharing information containing SSNs with marketing companies, collection agencies, credit bureaus, private investigators, and outside researchers.

Finally, few agencies reported that they place records containing SSNs on their Internet sites; however, this practice may be growing. Of those agencies that reported having public records containing SSNs, only 3 percent of the state respondents and 9 percent of the county respondents reported that the public can access these documents on their Web site. In some cases, such as the federal courts, documents containing SSNs are available on the Internet only to paid subscribers. However, increasing numbers of departments are moving toward placing more information on the Internet. We spoke with several officials that described their goals for having records available electronically within the next few years. Providing this easy access of records potentially could increase the opportunity to obtain records that contain SSNs that otherwise would not have been obtained by visiting the government agency.

While planning to place more information on the Internet, some courts and government agencies are examining their policies to decide whether SSNs should be made available on documents on their Web sites. In our fieldwork, we heard many discussions of this issue, which is particularly problematic for courts and recorders, who have a responsibility to make large volumes of documents accessible to the general public. On the one hand, officials told us placing their records on the Internet would simply facilitate the general public's ability to access the information. On the other hand, officials expressed concern that placing documents on the Internet would remove the natural deterrent of having to travel to the courthouse or recorder's office to obtain personal information on individuals.

Again, we found examples where government entities are searching for ways to strike a balance. For example, the Judicial Conference of the United States recently released a statement on electronic case file availability and Internet use in federal courts. They recommended that documents in civil cases and bankruptcy cases should be made available electronically, but SSNs contained in the documents should be truncated to the last four digits. Also, we spoke to one county recorder's office that had recently put many of its documents on their Web site, but had decided not to include categories of documents that were known to contain SSNs. In addition, some states are taking action to limit the display of SSNs on the Internet. Given the likely growth of public information on the Internet, the time is right for some kind of forethought about the inherent risk posed by making SSNs and other personal information available through this venue.

Concluding Observations

SSNs are widely used in all levels of government and play a central role in how government entities conduct their business. As unique identifiers, SSNs are used to help make record-keeping more efficient and are most useful when government enti-

[23] Some jurisdictions also permit citizens to request public records through the mail.

ties share information about individuals with others outside their organization. The various benefits from sharing data help ensure that government agencies fulfill their mission and meet their obligation to the taxpayer by, for example, making sure that the programs serve only those eligible for services. However, the gaps in safeguarding SSNs that we have identified create the potential for SSN misuse. Although the extent to which the government's broad use of SSNs contributes to identity theft is not clear, measures to encourage governments to better secure and reduce the display of SSNs could at least help minimize the risk of SSN misuse. It is important to focus on ways to accomplish this. We will be reporting in more detail on these issues at the end of this month and look forward to exploring additional options to better protect SSNs with you as we complete our work.

Contacts and Acknowledgments

For further information regarding this testimony, please contact Barbara D. Bovbjerg, Director, or Kay E. Brown, Assistant Director, Education, Workforce, and Income Security at (202) 512–7215. Individuals making key contributions to this testimony include Lindsay Bach, Jeff Bernstein, Richard Burkard, Jacqueline Harpp, Daniel Hoy, Raun Lazier, Vernette Shaw, Jacquelyn Stewart, and Anne Welch.

Appendix I: Examples of Federal Statutes That Authorize or Mandate the Collection and Use of Social Security Numbers

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Tax Reform Act of 1976 42 U.S.C. 405(c)(2)(c)(i)	General public assistance programs, tax administration, driver's license, motor vehicle registration	Authorizes states to collect and use SSNs in administering any tax, general public assistance, driver's license, or motor vehicle registration law
Food Stamp Act of 1977 7 U.S.C. 2025(e)(1)	Food Stamp Program	Mandates the secretary of agriculture and state agencies to require SSNs for program participation
Deficit Reduction Act of 1984 42 U.S.C. 1320b–7(1)	Eligibility benefits under the Medicaid program	Requires that, as a condition of eligibility for Medicaid benefits, applicants for and recipients of these benefits furnish their SSNs to the state administering program
Housing and Community Development Act of 1987 42 U.S.C. 3543(a)	Eligibility for HUD programs	Authorizes the secretary of the Department of Housing and Urban Development to require applicants and participants in HUD programs to submit their SSNs as a condition of eligibility
Family Support Act of 1988 42 U.S.C. 405(c)(2)(C)(ii)	Issuance of birth certificates	Requires states to obtain parents' SSNs before issuing a birth certificate unless there is good cause for not requiring the number
Technical and Miscellaneous Revenue Act of 1988 42 U.S.C. 405(c)(2)(D)(i)	Blood donation	Authorizes states and political subdivisions to require that blood donors provide their SSNs

Appendix I: Examples of Federal Statutes That Authorize or Mandate the Collection and Use of Social Security Numbers—Continued

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Food, Agriculture, Conservation, and Trade Act of 1990 42 U.S.C. 405(c)(2)(C)	Retail and wholesale businesses participation in food stamp program	Authorizes the secretary of agriculture to require the SSNs of officers or owners of retail and wholesale food concerns that accept and redeem food stamps
Omnibus Budget Reconciliation Act of 1990 38 U.S.C. 510(c)	Eligibility for Veterans Affairs compensation or pension benefits programs	Requires individuals to provide their SSNs to be eligible for Department of Veterans Affairs' compensation or pension benefits programs
Social Security Independence and Program Improvements Act of 1994 42 U.S.C. 405(c)(2)(E)	Eligibility of potential jurors	Authorizes states and political subdivisions of states to use SSNs to determine eligibility of potential jurors
Personal Responsibility and Work Opportunity Reconciliation Act of 1996 42 U.S.C. 666(a)(13)	Various license applications; divorce and child support documents; death certificates	Mandates that states have laws in effect that require collection of SSNs on applications for driver's licenses and other licenses; requires placement in the pertinent records of the SSN of the person subject to a divorce decree, child support order, paternity determination; requires SSNs on death certificates; creates national database for child support enforcement purposes
Debt Collection Improvement Act of 1996 31 U.S.C. 7701(c)	Persons doing business with a federal agency	Requires those doing business with a federal agency, i.e., lenders in a federal guaranteed loan program; applicants for federal licenses, permits, right-of-ways, grants, or benefit payments; contractors of an agency and others to furnish SSNs to the agency
Higher Education Act Amendments of 1998 20 U.S.C. 1090(a)(7)	Financial assistance	Authorizes the secretary of education to include the SSNs of parents of dependent students on certain financial assistance forms
Internal Revenue Code (various amendments) 26 U.S.C. 6109	Tax returns	Authorizes the commissioner of the Internal Revenue Service to require that taxpayers include their SSNs on tax returns

Source: GAO review of applicable federal laws

Appendix II: Our Eight Practices and How They Fit Into the Federal Framework for an Information Security Program

Certain federal laws lay out a framework for federal agencies to follow when establishing information security programs to protect sensitive personal information, such as SSNs.[24] The federal framework is consistent with strategies used by private and public organizations that we previously reported have strong information security programs.[25] This framework includes four principles that are important to an overall information security program. These are to periodically assess risk, implement policies and controls to mitigate risks, promote awareness of risks for information security, and to continually monitor and evaluate information security practices. To gain a better understanding of whether agencies had in place measures to safeguard SSNs that are consistent with the federal framework, we selected eight commonly used practices found in information security programs—two for each principle. Use of these eight practices could give an indication that an agency has an information security program that follows the federal framework.[26] We surveyed the federal, state, and county programs and agencies on their use of these eight practices:

Periodically assess risk

- Conduct risk assessments for computer systems that contain SSNs
- Develop written security plan for computer systems that contain SSNs

Implement policies and controls to mitigate risks

- Develop written policies for handling records with SSNs
- Control access to computerized records that contain SSNs, such as assigning different levels of access and using methods to identify employees (e.g., use ID cards, PINS, or passwords)

Promote awareness of risks for information security

- Provide employees training or written materials on responsibilities for safeguarding records
- Take disciplinary actions against employees for noncompliance with policies, such as placing employees on probation, terminating employment, or referring to law enforcement

Continually monitor and evaluate information security practices

- Monitor employees' access to computerized records with SSNs, such as tracking browsing and unusual transactions
- Have computer systems independently audited

Chairman SHAW. Thank you. Ms. Brown?

Ms. BROWN. I am here to answer——

Chairman SHAW. You are with Barbara Bovbjerg.

Ms. BROWN. Yes.

Ms. BOVBJERG. I brought reinforcements today.

Chairman SHAW. Good for you. We are delighted to have in you in Florida.

Ms. BOVBJERG. Thank you for inviting me.

Chairman SHAW. Lisa, you told a very compelling story with regard to your 3-year struggle. Has the defendant been adjudicated guilty or what has happened to the case?

---

[24] See federal Government Information Security Reform provisions of the fiscal year 2001 Defense Authorization Act, the federal Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and Office of Management and Budget guidance.

[25] U.S. General Accounting Office, Executive Guide: Information Security Management, Learning From Leading Organizations, GAO/AIMD–98–8 (Washington, D.C.: May 1998) reported on strategies used by private and public organizations—a financial services corporation, a regional utility, a state university, a retailer, a state agency, a nonbank financial institution, a computer vendor, and an equipment manufacturer—that were recognized as having strong information security programs. The information security strategies discussed in the report were only a part of the organizations' broader information management strategies.

[26] States may also require any number of the eight practices, but the requirements would vary from state to state.

Ms. TROPEPE. She received 4 months of in-house arrest, probation time, and community service.

Chairman SHAW. How about restitution?

Ms. TROPEPE. She surrendered the $10,000 cashier's checks that she got from my bank account, and the balance of the moneys were never—there was no restitution, none that I am aware of.

Mr. MORELL. I can give you a little bit of a backup on this, and we can—

Chairman SHAW. Excuse me, for the record, this is Mr. Tim Morell.

Mr. MORELL. Tim Morell, right. I am also the current co-Vice Chairman of the Computer Law Committee of the Florida bar, and we have been actively supporting and helping to get publicity for your bill, as you know from a year or two ago when I was in Del Ray helping out and trying to find out some information on this.

We were unable to get much of the prosecution at the State court level. It turned out that the only thing we could do was go to U.S. Attorney's Office. We were told that the amount of money involved, unless it was more than $100,000, wasn't going to get anybody's interest, so we ended up going to the media. We went to Channel 12, and we went to the Palm Beach Post. Once that was exposed, then the U.S. Attorney's Office took the case, and I have a copy of a Palm Beach Post summary that we can put into the record of what actually ended up happening. And I will read it if you would like to have that into the record.

Chairman SHAW. Without objection, I will place the entire Palm Beach Post article that you are holding into the record.

[The article follows:]

Palm Beach Post
West Palm Beach, Florida

WEST PALM BEACH—A temporary worker who stole the identity of a woman in her office, took $13,000 from her bank account and ran up $5,000 in credit card charges in her name was sentenced Friday to 4 years' probation and 150 hours of community service. Terkesha Lane 21, of Riviera Beach, faced up to 3 years in prison, a $25,000 fine and restitution. U.S. District Court Judge Daniel T.K. Hurley took note of Lane's age, her clean record and that she has a 2-year-old child. She also helped authorities track down a $10,000 cashier's check. "I think you earned this by everything else you have done in your life," the judge said. Lane who will be on home detention for the first 4 months of the probation and pay $100, apologized for the elaborate scheme in which she managed to obtain a driver's license in the name of Lisa Tropepe, withdrew money from Tropepe's bank account and ran up credit card charges in Tropepe's name. The bank reimbursed Tropepe and she restored her credit after hiring a lawyer.

Mr. MORELL. She was given, in summary, just 4 years probation and 150 hours of community service. There were some other monetary amounts here that we don't think will ever be collectable, but we will put this into evidence.

Chairman SHAW. Thank you. Mr. Ross, we will make available to you and Ms. Tropepe a transcript of this particular hearing that you can go in and show your creditors.

Mr. ROSS. Thank you.

Chairman SHAW. That you have appeared before a congressional Committee who is studying the tragedy of identity theft. Mark?

Mr. FOLEY. Well, I think this illuminates the problem. In addition to having to go through hours, now we have got a lawyer and an engineer, both professionals who have both competence and ability to probably pursue this. Think about a poor person who is just struggling?

Ms. TROPEPE. That is right.

Mr. FOLEY. And this is outrageous. And 4 years probation to steal how much, $40,000?

Ms. TROPEPE. Over $20,000.

Mr. FOLEY. Plus, plus.

Ms. TROPEPE. Plus, plus.

Mr. FOLEY. I mean with credit damage and all.

Ms. TROPEPE. That is not including the cost to the firm, myself, the cost to hire Tim Morell to clear my name. It is not including all that.

Chairman SHAW. But the bank they made good on your account, didn't they?

Ms. TROPEPE. The bank made good on the account, and the credit cards that she received or the instant credit that she received, the credit companies, they paid for that as well. So there was no out-of-pocket money, but all the other—the attorney and the time and the grief that it has caused my office. I was in the process of becoming a partner, and checking my billable time was slowly declining every day, and I just wasn't functioning right. And then we finally hired an attorney that helped alleviate that, but I can tell you that there isn't a day that doesn't go by that I don't think about the fact that there is somebody around that is right up the street from me that can do it again. And if she doesn't do it, she has the information still to this day to give it to somebody else. It just doesn't seem to me—the punishment, without a doubt, does not fit the crime.

Mr. FOLEY. That is where I see we have two problems. We have, one, punishment, because if you can get away with the kind of larceny that has occurred with that minimal sentence, it encourages people to go ahead and try. Secondly, if you can't protect the Social Security Numbers, it is a catch-22.

Ms. TROPEPE. Right.

Mr. FOLEY. So you are around and around in circles on this issue.

Mr. MORELL. This file represents a lot of effort here to try to keep Lisa's credit in decent shape. She continues to have—a lot of the times we try to keep this so that it doesn't bother her, but as recently as 6 months ago her identity was compromised in, what was it, Ireland or somewhere in the British Isles. Somebody had compromised her identity mostly because once it happens once and you are out there, then there is almost like the reasonable doubt, it would be hard to prove who the criminal was after that. And so they go for you. And that was one of the reasons why we were very nervous about even coming here today. The thing keeps coming back, and the nature of computers is such that once the record is out there somebody inadvertently enters it again or it comes back up in 6 months, and it is all right back like it never left. And it has been a constant struggle to try to keep after those credit bureaus, to keep telling them Lisa is not the perpetrator.

Mr. FOLEY. The other problem is the credit reporting. When you go now to a store you—and I probably can't take advantage of these instant credit opportunities——

Ms. TROPEPE. Never again.

Mr. FOLEY. Because we will always be——

Ms. TROPEPE. Right.

Mr. FOLEY. On somebody's list that they have to flag, that they have to check, that they have to make sure you are who you are for our safeguard, but nonetheless it inconveniences us.

Ms. TROPEPE. Right. Well, there is a fraud alert on my name, so I will never be able to get instant credit again. I will have to go through the longer process in order to obtain a credit card for the rest of my life. And this all started with her getting my Social Security Number on the Internet.

Chairman SHAW. Did she get it out of the payroll records of the company or——

Ms. TROPEPE. No. She told me that her cousin in Miami helped her get it off the computer.

Chairman SHAW. Oh, you talked to her about it since she was charged.

Ms. TROPEPE. Well, I am the one who solved the crime. I went to my ATM machine and sometimes you can't tell when a couple dollars are missing, okay? But it was $13,000 subtracted out of my account, which alerted me that night. So the very next day I called up First Union and said, "What is happening to my account?" Meanwhile, I am getting every day credit card bills in the mail on a daily basis that I knew nothing about. They told me that I withdrew a $10,000 cashier's check 2 days prior at the Okeechobee Boulevard branch in West Palm Beach, and I said I have never been to the Okeechobee Boulevard branch in West Palm Beach. I drove over there and they replayed the tapes from the bank, and I identified her on those bank tapes. If she had not gone to the bank and started withdrawing cash from my account, I would have never found out who the perpetrator was.

And then after that she said to me that she also did—you know, you kind of figure that, okay, since she has taken money out of my account she is probably doing the credit cards too. And I asked her and she said, "Yes, I did that too." "And how did you do it?" "I got your Social Security Number from my cousin in Miami who looked it up on the Internet."

Chairman SHAW. What site?

Ms. TROPEPE. So that is how it started. And then once she had that, she had my home address because she was our receptionist. She took those two pieces of information to DMV, the Division of Motor Vehicles, received a driver's license with my name, address, and information and her picture.

Mr. MORELL. That is what I wanted to follow up with. By having the Social Security Number, she was able to get a duplicate driver's license, although our system in Florida has a picture ID. They could have clearly seen the woman who impersonated her looks nothing like Lisa, nothing at all physically. But they had her picture there, but it didn't matter what the picture was. Because the woman had Lisa's Social Security, they gave this woman a driver's license and that became the key to everything.

Ms. TROPEPE. And the Division of Motor Vehicles did have my picture on file because, as you both probably know, I was a Broward County resident until about 4 years ago. I went to the Division of Motor Vehicles, got a new driver's license, so my picture was on file in Palm Beach County. They just never bothered to look at my picture when they gave her the duplicate driver's license.

Mr. FOLEY. Anthony, why don't you tell us about some of the late night calls during these periods after your credit has been run up.

Mr. ROSS. Late night calls?

Mr. FOLEY. Collection agencies, people. I mean this is the other side of it you don't realize.

Mr. ROSS. Well, as a Federal Law Enforcement Officer and I teach at the Federal Law Enforcement Training Center in Brunswick, Georgia, and we are on a 6-day work week right now. And that and family obligations and just trying to live on that extra day I get off and deal with these has just been a nightmare. And what happens is you receive—if you send in the proper paperwork to try to get this cleared with a creditor, they have a certain number of days that they are looking to have you respond in. And that is not always necessarily possible, especially traveling and other things that do occur within the job. So then you get another letter saying, "Well, it appears since you have not sent the paperwork in that you no longer want to pursue this and that you are the person that has made these charges, and now this bill is yours, basically."

Now you have to go back and call, "I do want to pursue this. I am just not able to do it in your time requirements, and now we are starting all over again." Or I have had instances where they have closed it out and I will say, "I haven't received anything more on this." "Well, we didn't get that back in time." Or I have had situations where you may have certain stores that use one banking institution or credit company that supplies credit for all of them. Now you have three different—in this case, I have three different fraudulent accounts, but it was backed by one creditor. Rather than them combining that as one fraudulent account, I had to submit documents individually for each one, and then they assigned them to three different fraud investigators within this one company. So instead of dealing with it one time, I had to deal with it multiple times.

One of the other problems that I came into, and this is a situation within the prison system is that the actual main person involved in this case that was orchestrating the fraud was already in custody, and he was using other family members and giving them the information on how to proceed along the fraud.

Mr. FOLEY. So he is inside working outside.

Mr. ROSS. Right.

Chairman SHAW. Absolutely amazing. I will share with you a story that we had in Washington. One of the Members of the Committee on Way and Means, Sam Johnson, who was a prisoner of war for, I think, 7 or 8 years at the Hanoi Hilton in Vietnam, and I had to tell him that—I said, "Your serial number and rank and those things that you give as a prisoner of war, your serial number is your Social Security Number, and we are trying to get away from that." I said, "All those people that were looking over you in

prison have your Social Security Number." But I think our military is backing away from that too, and we have got to be terribly careful.

And then we had a colonel who testified before us, and he was cashing a check at the PX, and he had to put his ID number on it and that was his Social Security Number, and that is where they picked his up. But you, you were quite correct to say that if you know how to find it, you can find it on a computer and people are—there is trafficking in these numbers. And that is what we have got to—that is what we have really got to stop.

It is not all together when you think that the logic of this thing is to get rid of it, but there is a number of organizations that are not in favor of this type of legislation, who deal in identities, whether they be private detectives or whatever, but the type of legislation that we are trying to develop is one that preserves the legitimate government use of the Social Security Number. It was never meant to be a national ID number, but it has sort of risen to that, and it is done without adequate protection. And this is what you people have run into.

And I am quite impressed with what the State of Florida has done in this regard. We are trying to move this legislation through several Committees. We moved it through the Committee on Ways and Means in the last Congress but it got stuck in a couple of other Committees with jurisdiction. We are trying to go back and maybe just work the bill so it is the jurisdiction of the Committee on Ways and Means so we can go ahead and pass it and then if they want to go forward with another bill, that they can do that or they can get moving and get the thing done on—get it done on their own Committee because this is terribly important that people like you go through this just because we, the people who issue the numbers, haven't put the proper safeguards in place in order to protect you from identity theft, when you have no choice but to go with a Social Security Number.

Also, as you did with the driver's license, we need to also put some type of a code as to someone's nationality. You come here as a citizen of another country, even if you don't have a work permit, if you have a bank account or if you are a student here on a student visa, you have to have a Social Security Number before you even open a bank account. Well, we need to put some identifier on that so that the Social Security Number that is given out will indicate that this person is not a citizen and this person is here on a certain kind of visa. And you can do it simply by just adding a letter from the alphabet on that, and that is another matter that we are looking into. Anything further, Mark?

Mr. FOLEY. I just wanted to thank Ms. Dykas for many things, obviously being here today and for your help on Good Sams St. Mary's for leading that effort and as well as Manora Gardens.

What is the State doing that you find successful as a mode for other States, and what do you think the Federal government should do to help with this effort of identity theft?

Mr. DYKAS. I think that the State being on the forefront, unfortunately, of having probably one of the highest rates of identity theft and certainly post-September 11 issues empanelled a grand jury, as I indicated, that that grand jury was in place for well over

6 months and was able to take testimony similar to the panel today and get very real life experiences as well as talk with experts in terms of crafting some type of resolution. And the grand jury report that came out on January 10, if you split it in two categories, dealt largely with recommendations to Florida Department of Highway Safety and Motor Vehicle in terms of the driver's licenses, certainly being a port State that we have a large influx of people from other countries, and dealing with those issues that may be more unique to a Florida, California, Texas.

It is an issue that I think everybody recognizes is a problem. But if you identify what issues you can deal with, those issues that how do we help the victims after it has occurred, and I think the focus now with regard to the legislation is how do we prevent it from happening? And I think it is particularly tricky with all of the clerk's offices, for instance. Many of the lawyers that deal with them are all going to electronic filing, electronic posting, me being a State of Florida employee, all of my information is public record, including my Social Security Number. So they are working on getting those issues exempted out as well.

Mr. FOLEY. Thank you.

Chairman SHAW. You just said something that rings an alarm in my head that what can we do, the Federal government, after you have been victimized to see that you don't go through this. The issuing new Social Security Numbers really isn't the answer, because that goes back and then some will have trouble with all the earnings that they have had. But that is something that we need to take up with the Social Security Administration—what do you do once someone has been victimized? Because, Lisa, you are quite right, you are more vulnerable because you have been already violated, and it is important, I think, that we look into this and see what can be done. Ms. Bovbjerg just made a note, so that must mean I said something that she is going to look into, I hope.

Mr. DYKAS. Well, I will give you one. Having been in the Economic Crime Section here, it is very tough sometimes to get a second Social Security Number, because frequently that is what credit repair scams do. They suggest that you get a new Social Security Number if you were actually the one who truly did have a bad credit as a way to avoid any type of proper credit reporting. So you bump up against issues all along the way.

And one last comment I would suggest to this panel as well is we have heard individual stories but part of what was submitted from our office was also the cost to businesses, banking entities as well. Two items briefly: Visa, in 1997, had a total of $490 million in losses; Master Card, in 1997, had $407 million in losses. So it affects everyone.

Chairman SHAW. That was from identity theft?

Mr. DYKAS. Yes.

Chairman SHAW. Wow.

Mr. DYKAS. Yes.

Chairman SHAW. They are getting half a billion dollars. Thank you all. Thank this panel very much, and we very much appreciate you taking the time to come down here and share your experience with us.

Lee Cohen, the Assistant State Attorney in Charge, Misdemeanor Trial Unit, State Attorney's Office, 17th Judicial Circuit of Florida, Broward County, Florida. We have——

Ms. GUIALDO. Anthanagtha Guialdo.

Chairman SHAW. Thank you. Say it again for me, please.

Ms. GUIALDO. Anthanagtha Guialdo.

Chairman SHAW. Anthanagtha.

Ms. GUIALDO. Guialdo.

Chairman SHAW. Guialdo. Legal Assistant in Charge of Identity Theft Unit, the State Attorney's Office, also with the 17th Judicial District of Florida from Broward County; the Honorable Ed Bieluch, who is Sheriff with Palm Beach County, West Palm Beach, Florida; and Paul Rispoli, who is the Sergeant of Palm Beach County Sheriff's Office in West Palm Beach; and Roland Maye, Special Agent-in-Charge, Atlanta Field Division, the Office of Inspector General, the Social Security Administration in Atlanta, Georgia.

I want to thank all of you for being here. We have your written testimony. It has been submitted, it will be made a part of the record, and you may proceed as you see fit.

Mr. Cohen.

STATEMENT OF LEE COHEN, ASSISTANT STATE ATTORNEY IN CHARGE, MISDEMEANOR DIVISION, STATE ATTORNEY'S OFFICE, 17TH JUDICIAL CIRCUIT OF FLORIDA, BROWARD COUNTY, FLORIDA

Mr. COHEN. Good afternoon, Mr. Chairman, Congressman Foley. On behalf of Michael J. Satz, State Attorney, Broward County, I would like to thank you for inviting us to be here. I am the Assistant State Attorney in Charge of the Misdemeanor Division, and I have the pleasure of also supervising Ms. Guialdo, who is our Identity Theft Unit Legal Aide there in that unit. I would like to bring a little bit different perspective to your proceedings, because I am sure you have been inundated with stories, as we have heard today, about financial losses, economic fraud, identity theft, credit card scams and the like. In our unit, we handle things—we have a little bit different twist on what happens with identity theft involving Social Security Numbers.

Just a little background. Before I came to my current position, which I have had for about 5 years, I was a Prosecutor in our Elder Abuse and Exploitation Unit. And there I was charged with dealing with crimes against the elderly and the senior citizens of Broward County involving fraud and exploitation. Most of the cases I dealt with were care giver type of relationships, between care givers and the seniors they were supposed to be caring for. It was very common at that time for me to have cases where credit card applications were redirected or intercepted by the care givers. And I think that puts them in a key position for this type of identity theft above and beyond your normal relationship or normal mail situation.

Most people do get their mail. The seniors that are being cared for by the care givers are having their mail intercepted. So I was having cases where the care giver would get the application, fill out the application, get the credit cards or add their names to other

people's credit cards, and continue on this type of fraud on and on for a very long period of time without detection because the senior citizen was not getting their mail. It wasn't until years later sometimes where family Members got involved where this was detected. So I would like you to consider in your deliberations the effect that the elderly have because of their having to rely on others for their mail which is their main line of communication.

One of the recommendations I had at various hearings and meetings with different participants from the security agencies of the financial institutions was to advocate and strengthen the fraud alerts on the accounts as well as putting certain restrictions on the accounts where you can call the bank and say, "I do not want anybody adding their name to my account. I do not want any changes to the account without a personal contact to me over the telephone with certain information provided." I think that would be helpful, and I always advocate that the victims I dealt with were citizens that I spoke to to do such a thing. And I think also any—obviously, I know that restricting the mailing out of applications and offers is a controversial issue, but I think that whatever can be done I that would be helpful.

The Identity Theft Unit that we have in the County Court Division is a very unique but, believe it or not, longstanding division that Mr. Satz has had since approximately 1978. There we have a unit that is devoted to what we used to call, or still called by many, the "not me" cases, where somebody is charged with a crime or a person is charged with a crime, a name is charged with a crime. The person comes to court and they say to the judge or they say to their attorney or they say to the prosecutor, "That wasn't me." And of course the response is, "Yes, sure. Tell it to the judge or tell it to the lawyer."

But these are not cases of mistaken identity like, "I was at home eating mashed potatoes with my wife." These are cases where this is not the person that the police intended to arrest or intended to bring into the system. Somebody else has used their name during an encounter with law enforcement which has caused the innocent person to now be charged with a crime or dealing with the criminal justice system.

And Ms. Guialdo is here to tell you a little bit about how she deals with those cases. She deals with a large number of those cases per year, most of the time dealing with driver's license and driving offenses. Thank you.

STATEMENT OF ANTHANAGTHA GUIALDO, LEGAL ASSISTANT, IDENTITY THEFT UNIT, COUNTY COURT DIVISION, STATE ATTORNEY'S OFFICE, 17TH JUDICIAL CIRCUIT OF FLORIDA, BROWARD COUNTY, FLORIDA

Ms. GUIALDO. Hello, Mr. Chairman, Mr. Foley, nice to meet you. My name is Ann Guialdo. I am a Legal Assistant with the 17th Judicial Circuit, the Identity Theft Unit. As Mr. Cohen stated again, our unit deals basically with an accused victim who may or may not have been arrested but an original arrest was made by somebody using their names or they were booked using that person's name but the accused was arrested.

So my job is to go back within the file and check the original arrest, fingerprints if there are any, booking photos if there are any, and clear up the accused's name. Most of the time it is a notice to appear where John Brown gives Tom Brown's name and says Tom Brown's Social Security. He might know it from speaking with Tom Brown is related to Tom Brown. So there that Social Security problem comes in where we have to go in and clean up Tom Brown's Social Security and personal information from John Brown's name. So it becomes a big issue all the time, because when someone is arrested their Social Security automatically is put on the probably cause affidavit. So we always come into that Social Security problem used as an identifier.

My duties include determining whether this office charges the right person by initiating an investigation into prosecuting those who unlawfully use the identities of others. The most prevalent cases I deal with are driving offenses wherein a suspect comes to the unit claiming that they hadn't received a citation but that somebody else did. It is our job to look into it, be it by signatures or identifiers from a driver's license that doesn't match that of the accused and find out really who did it.

We also have felony cases where somebody is incarcerated under my name. It is my job now, because this person is already in the prison systems, to correct that information so by the time this person gets paroled that he will come out in his own name and not that of the accused. So we have a big process in investigating that with fingerprints, Florida Department of Law Enforcement (FDLE), the Federal Bureau of Investigation, and the prison system in just trying to correct identifiers.

A lot of times we have cases where I go in for a background check and because somebody used my name or somehow the Social Security Number the imposter gave was wrong, it becomes my problem because it was my Social Security Number. And my name is now on their criminal history. So it becomes a problem trying to clear all of that off and putting it on the right person. I had placed into evidence exhibits, so those are basically the things—it is a process. We have walk-in complaints, phone calls and mail from all over the country.

My, not really recommendation, but fingerprints and Social Security should kind of go hand in hand as identifiers. There should be a way where a fingerprint could match a Social Security Number or something, because, you know, criminals are out there, and they do it every day. I had a lady call in, I was trying to help her. She came in, filled out her paperwork and everything, and she called the imposter's job, said she was me, and the only way to distinguish that it wasn't me is you can notice my name, and she couldn't spell it.

Chairman SHAW. I couldn't pronounce it.

[Laughter.]

Ms. GUIALDO. It is hard. So, you know, it becomes a problem for everybody. Lately, I have been having a lot of Social Security calls. Mothers call up and say, "My son is going to go to school in September. I need to get a Social Security Number. Well, I went to the Social Security Administration, they told me he already has a Social Security Number." And they do a printout and here it is.

Well, the father is using the Social Security—received a Social Security Number in the child's name. So now she has to do whatever to try to straighten that out.

Chairman SHAW. Yes, but I think you have to do it in the hospitals now.

Ms. GUIALDO. Right. So the father is using it, so it becomes a whole problem for this child. It is very difficult. I have had—my brother's name is similar to mine, we are a number off, so that becomes a problem also, because when law enforcement is putting it in their system, somebody is manually putting them in. A number is off. It automatically becomes my problem. So it a catch-22 issue. Thank you.

[The prepared statement of Ms. Guialdo follows:]

Statement of Anthangtha Guialdo, Legal Assistant, Identity Theft Unit, County Court Division, State Attorney's Office, 17th Judicial Circuit of Florida, Broward County, Florida

My name is Anthangtha Guialdo and I am a Legal Assistant assigned to the Identity Theft Unit within the County Court Division of the Office of the State Attorney, 17th Judicial Circuit in Broward County. Assistant State Attorney In Charge Lee G. Cohen and I have been asked by State Attorney Michael J. Satz to represent this office at this hearing. The Identity Theft Unit, originally referred to as the "Not Me" Unit, was created by Mr. Satz in 1978 to assist those whose identities have been misused in criminal cases. I have been working in this unit for 5 years. This unit processes approximately 2400 cases each year.

A majority of the cases presented to me are done so by the accused (currently named defendant) wherein they are claiming that they have been mistakenly accused of a crime when in fact law enforcement or the Office of the State Attorney intended to charge someone else (often referred to as a "Not Me" case). This is due to the true perpetrator using the name or otherwise identifying him or herself as the accused. The perpetrators are usually family members or acquaintances of the accused or strangers who have gained access to personal information of the accused. I have even had my identity stolen by one of the accused that I was trying to help but as you can imagine, she had difficulty in determining the correct spelling of my name.

My duties include determining whether this office charges the right person as well as initiating investigations into prosecuting those who have unlawfully used the identities of others. The most prevalent type of cases I deal with are driving offenses wherein a suspect comes to this unit claiming that they received a citation for a criminal or civil traffic offense in their name and that in fact, they were never stopped for such offense. Other misdemeanor and felony cases are also presented where the currently charged defendant claims "Not Me." When a defendant begins to claim that there has been a mistaken identity as to who committed the crime or poses an alibi (i.e. "It was me who they arrested but I didn't do it"), that defendant is immediately referred to his or her lawyer for further legal advice.

When processing a case in this unit, I will interview the suspect and obtain as much personal documentary information I can including fingerprints, signatures, and copies of driver's license. I will then obtain records and photographs from several agencies including the Department of Highway Safety and Motor Vehicles and the local police agencies as well as have fingerprint comparisons made. Occasionally officers or witnesses will be asked to come to the office to see if identifications can be made in order to determine true identities. If I determine that the wrong person is accused then recommendations are made to the Assistant State Attorneys for the charges to be dismissed. If the identity of the true perpetrator is determined, orders and corrected charging documents will be drafted reflecting the correct person's identity as well as the charging of additional criminal charges pursuant to F.S.S. 817.568 for Criminal Use of Personal Identification Information, F.S.S. 843.02 Resisting/Obstructing Officer without Violence and F.S.S. 831.01/831.02 Forgery. (See "Exhibit A")

In processing my cases, I rely heavily on the validity of Social Security numbers. For example, when checks are made through the National Criminal Information Services and the Florida Criminal Information Services the Social Security number is linked to the master (true) name as an identifier, as well as listing all alias names, dates of birth and Social Security numbers. (See "Exhibit B") Additionally, during the booking process, and more importantly for me (due to no fingerprinting of photographing of the suspect), during the issuing of a Notice to Appear/Citation in place of booking, the suspect is often inquired as to his or her Social Security number, which can later be used to verify or distinguish identity. (See "Exhibit C") The Social Security number is also used to verify the accuracy of the transposition of names from person to document and document to document, as well as being used to distinguish between persons with common names. (See "Exhibit D") Our Information (charging documents) even lists the Social Security number on the top for identification purposes. (See "Exhibit E")

State Attorney Michael J. Satz conveys his appreciation for requesting input from this office in this matter. Anything that can be done to insure the validity of Social Security numbers will assist in this unit's goal to ensure that only the correct de-

fendants are charged with crimes and to assist those victims of the system who are mistakenly charged due to the criminal acts of others.

Chairman SHAW. Thank you. Sheriff?

STATEMENT OF HON. ED BIELUCH, SHERIFF, PALM BEACH COUNTY, WEST PALM BEACH, FLORIDA

Mr. BIELUCH. Good afternoon. Let me preface this by saying that I am not an expert in identity theft; however, it has been around longer than I have been in law enforcement, as Ms. Guialdo stated, particularly with drivers' licenses, and we have had to deal with that over the years many, many, many times, and what we do is if we have someone that is driving with no identification, then we take a thumbprint on a special piece of paper and attach it to the citation so that they can be identified later in court should somebody show up and say, "It wasn't me."

It seems like that would be impractical in dealing with a Social Security card unless there was some type of electronic reader that could do the reading and compare them, which I suppose there is. I mean there is all kinds of identifiers out there—iris identifiers and that type of thing—which will probably help at some point when we get to that technology. I mean technology is kind of the catalyst here. Technology has allowed identity theft to really, really grow, and it is probably going to be the way that we have to solve it.

Couple points I will make on what Mr. Morell said earlier, that the amount of money seeming to stymie the investigation, and I think that is very true, that $20,000 in the overall scheme of things isn't a lot of money but really it is. And, you know, we look at these at property crimes as opposed to person crimes where somebody is injured, but in many cases I believe that these are almost life threatening because some people just can't afford to lose $20,000. I mean to some people it is a drop in the bucket, but others that is their life, and that is their college money, that is their retirement money, it is whatever they have been saving up for for dozens and dozens of years. And it is almost a life threatening crime to them, and I think we need to approach it on a more serious level regardless of the amount.

And one of the other problems is when we talk about trying to get people back on track and get back in the system, and it seems like a lot of red tape, and I am sure it is, but there are thousands, millions of people out there who are genuine bad guys. They are ripping off stores with credit cards and that type of thing, so I mean the other side of the coin is that that is what they are up against when they go to have their credit restored is the fact that there are lots of bad people out there and they just don't believe their story. But I am going to let Sergeant Rispoli talk because he is our expert on identity theft.

STATEMENT OF PAUL RISPOLI, SERGEANT, PALM BEACH COUNTY SHERIFF'S OFFICE, FINANCIAL CRIMES UNIT, WEST PALM BEACH, FLORIDA

Mr. RISPOLI. Good afternoon, Mr. Chairman, Mr. Foley. On behalf of Sheriff Bieluch and the entire Palm Beach County Sheriff's Office Financial Crime Unit, I want to thank you for inviting us today. My name is Sergeant Paul Rispoli. I am currently in charge of the Palm Beach County Sheriff's Office Financial Crime Unit. Also here with me today is my Captain, Captain Simon Barnes from the Detective Bureau, along with two detectives from the unit: Detective Alice Gold and Pete Palenzuela. Any questions I can't answer they will be able to answer.

Detectives in the Financial Crime——

Chairman SHAW. But they are sitting in the back and said you are on your own.

[Laughter.]

Mr. RISPOLI. I didn't see the door shut, so I know they are still here. Detectives in the unit are responsible for the investigation of white collar crimes, specifically responsible for investigating exploitation of the elderly, corporate embezzlement, identity theft, credit card fraud, counterfeiting and computer Internet fraud. This six-person unit shares a combined 100 years experience in law enforcement. During this time, we have been assigned to road patrol, different units within the Detective Bureau, along with money laundering.

Of all the crimes I have investigated personally, identity theft cases are one of the most difficult. They are difficult in identifying the suspects, difficult to get financial institutions to cooperate, difficult to prosecute and difficult to have the guilty parties receive sentences that would deter committing identity theft again. Over the past 5 years, there has been a significant increase in crimes where criminals compromise personal identification data of victims in order to commit identity theft. The information falling into criminal hands includes name, date of birth, Social Security Number, banking account numbers, and other financial information.

The victims of identity theft, like other crimes, are made to feel personally responsible. This is especially true in light of the vicious cycle of events following the circumstances of the crime. Imagine for a moment, which Mr. Foley has already run into, you go to a car dealer to buy a new car only to be denied because of a negative payment on your credit report—information that you had no knowledge of. The trauma this type of fraud causes its innocent victims is inconceivable, as victims are usually left to fix the problem.

I will explain some of the difficult areas involved with investigating identity theft. Identifying the suspect. Technology, as the Sheriff has said, has improved a thief's chances of getting away with crime. A thief doesn't need a gun or a mask to commit a crime. Today's gun is a keyboard and the mask is a computer with Internet access. You can apply for loans, credit cards, bank accounts online. You can purchase items with a click of a button and have them shipped all over the world. The thief is never seen. The credit cards and the merchandise is delivered to an empty apartment in the thief's building or neighborhood or a post office box under the victim's name. Most financial institutions and credit card

companies fail to check or question why the applicant's address is different than the address listed in the credit report.

Most of our complaints come from victims who are local and the thief is in another country, State, or county. Florida has a statute dealing with this crime. The statute allows for a venue for the prosecution and trial of violations to be commenced and maintained in any county in which an element of the offense occurred, including the county where the victim generally resides. The local law enforcement agency where the victim resides does not normally have the ability and resources to investigate the offense when it occurs in another county or State.

Financial institutions' and credit card companies' cooperation—most financial institutions and credit card companies are reluctant to cooperate during an investigation, because it generate negative publicity, and the loss amount on one case is usually not enough to begin an investigation. It costs more to investigate the case than write off the loss. That is what I have been told.

Prosecution and sentencing. Even when a thief is identified and there is probable cause for arrest, some prosecutors tend to plead a case out prior to trial. This plea agreement is usually probation and restitution. When criminals have been found guilty in court, they rarely see any jail time. Most are sentenced to probation and restitution anyway, so there is no deterrence to committing this crime.

Financial and white collar crime has always been viewed as a lesser threat than a burglary or a robbery. Common consensus is no one is hurt. Ask a victim of identity theft is they feel any less violated than a robbery victim or a burglary victim. Victims have been refused employment, loans, some victims have actually been arrested for crimes that the identity thief has committed. Victim lives have been destroyed in this crime. In light of the events of September 11, 2001, one should be aware that identity theft in Florida played an important role in a terrorist being able to carry out their objectives. Identity theft does hurt people.

Some recommendations suggested by the Palm Beach County Sheriff's Office Financial Crime Unit: An increase in public education about identity theft, which this is part of, the media is all gone now but at least they were here; increased law enforcement education and interagency cooperation. Victims should not be turned away; a report must be taken. The current identity theft statute needs to be updated with enhanced penalties for this crime. This will make the crime less attractive for a thief.

Credit cards and financial institutions should be held responsible for indiscriminate issuing of credit to unauthorized persons, i.e, mass mailing pre-approved credit applications. Credit bureaus must take a more active role in ensuring security of one's credit. This may involve notifying a person that their credit has been checked. Also, I heard, I am not sure which panelist it was, said about the fraud alert. That doesn't live with you the rest of your life unless you keep on calling. After a certain amount of time, each credit bureau can shut that off.

Require any web-based company or company taking credit applications over the Internet to maintain detailed records of their transactions. Posting of Social Security Numbers on the Internet

should be prohibited. Entities having access to a consumer's personal identifying information should be strictly accountable as to whom they provide such information to and the purpose the information is being provided for.

We believe if there were an enhancement to the penalties for identity theft, the criminal element would less likely attempt to commit this crime.

In closing, we would like to thank you, Congressman Shaw and Mr. Foley, for giving law enforcement an opportunity to offer input into this matter. Additionally, we would ask that this Committee consider the massive impact identity theft has had on our society. Thank you.

[The prepared statement of Mr. Rispoli follows:]

Statement of Paul Rispoli, Sergeant, Palm Beach County Sheriff's Office, Financial Crimes Unit, West Palm Beach, Florida

Good Afternoon, Mr. Chairman and members of the Subcommittee. On behalf of Sheriff Ed Bieluch, we would like to thank you for the opportunity to appear before you today to discuss this very important subject.

My name is Sgt Paul Rispoli. I am currently in charge of the Palm Beach County Sheriff's Office Financial Crimes Unit Seated next to me is the Sheriff of Palm Beach County Ed Bieluch, Captain Simon Barnes and Detectives Pete Palenzuela and Alice Gold.

We are currently assigned to the Financial Crimes Unit. Detectives in the Financial Crimes Unit are responsible for the investigation of white-collar crimes, specifically responsible for investigating **exploitation of the elderly, corporate embezzlement, identity theft,** credit card **fraud, counterfeiting and computer Internet fraud.**

This six-person unit shares a combined 100 years experience in law enforcement. During this time, we have been assigned to road patrol, different units within the detective bureau itself and money laundering.

Of all the crimes I have investigated, identity theft cases are the most difficult.

- Difficult in identifying the suspect(s),
- Difficult to get financial institutions to cooperate,
- Difficult to prosecute, and
- Difficult to have the guilty parties receive sentences that would deter committing identity theft.

Over the past five years, there has been a significant increase in crimes where criminals compromise personal identification data of victims, in order to commit identity theft. The information falling into criminal hands includes:

- Name,
- Date of birth,
- Social Security Number,
- Banking account number, and other personal and financial information.

Victims of identity theft, like other crimes, are made to feel personally responsible. This is especially true in light of the vicious cycle of events following the circumstances of this crime. Imagine for a moment, you go to a car dealer to buy a new car, only to be denied because of a negative payment history reflected in a credit report—information that you knew nothing about. The trauma this type of fraud causes its innocent victims is inconceivable, as victims are usually left to fix the problem.

I will explain some of the difficult areas involved with investigating Identity Theft——

Identifying the syspect:

Technology has improved a thief's chances of getting away with crime. A thief doesn't need a gun or a mask to commit crimes. Today's gun is a keyboard and the mask is a computer with Internet access. You can apply for loans, credit cards, and bank accounts online. You can purchase items with the click of a button and have them shipped all over the world. The thief is never seen. The credit cards and merchandise is delivered to an empty apartment in the thief's building or neighborhood or a post office box under the victim's name.

Most Financial institutions/Credit Card companies fail to check or question why the applicant's address is different than the address listed in the credit report.

Most of our complaints come from victims, who are local and the thief is in another county, state, or country.

Florida has a statute dealing with this crime. The statute allows venue for the prosecution and trial of violations to be commenced and maintained in any county in which an element of the offense occurred, including the county where the victim generally resides.

The local law enforcement agency where the victim resides does not normally have the ability and resources to investigate the offense when it occurs in another county or state.

Financial institutions and Credit Card Companies cooperation:

Most financial institutions/credit card companies are reluctant to cooperate during an investigation because it can generate negative publicity. The loss amount on one case is usually not enough to begin an investigation.

It costs more to investigate the case than to write off the loss.

Prosecution and Sentencing:

Even when a thief is identified and there is probable cause for an arrest some prosecutors tend to plea a case out prior to trial. This plea agreement is usually probation and restitution. When criminals have been found guilty in court they rarely see any real jail time. Most are sentenced to probation and restitution anyway, so there is no deterrence to committing this crime.

Financial (white collar) Crime has always been viewed as a lesser threat than a burglary or a robbery.

Common consensus is **"No one is hurt".**

Ask a victim of identity theft if they feel any less violated.

Victims have refused employment, loans, and some victims have actually been arrested for crimies the identity thief has committed.

Victim's lives have been destroyed by this crime.

In light of the events of September 11, 2001, one should be aware that identity theft in Florida played an important role in the terrorist being able to carry out their objectives.

Identity Theft does hurt people in many ways.

Some Recommendations suggested by the Palm Beach County Sheriff's Office Financial Crimes Unit:

- Increase Public education about Identity Theft.
- Increase Law Enforcement education and interagency cooperation. **Victims should not be turned away—a report must be taken.**
- The current Identity Theft statute needs to be updated with enhanced penalties for this crime. This will make the crime less attractive for a thief.
- Credit card companies and Financial Institutions should be held responsible for indiscriminate issuing of credit to unauthorized persons. (Mass mailing pre-approved credit cards to the public)
- Credit Bureaus must take a more active role in ensuring security of ones credit. This may include notifying a person that their credit has been checked.
- Require any web-based company or company taking credit applications over the Internet to maintain detailed records of their transactions.
- Posting of Social Security Numbers on the Internet should be prohibited.
- Entities having access to a consumer's personal identifying information should be strictly accountable as to whom they provide such information to and the purpose the information is being provided for.
- We believe if there were an enhancement in the penalties for identity theft, the criminal element would less likely attempt to commit this crime.

In closing, we would like to thank Congressman Shaw for giving Law Enforcement an opportunity to offer input in this matter. Additionally we would ask this committee to consider the massive impact identity theft has had on our society.

Chairman SHAW. Thank you. Mr. Maye?

STATEMENT OF ROLAND MAYE, SPECIAL AGENT–IN-CHARGE, ATLANTA FIELD DIVISION, OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, ATLANTA, GEORGIA

Mr. MAYE. Good afternoon, Congressman Shaw and Congressman Foley, and thank you for inviting the Office of the Inspector General, the Social Security Administration to testify today. My name is Roland Maye, and I am the Special Agent-in-Charge of the Criminal Investigative Activities for this region.

As you noted in your opening remarks, the misuse of Social Security Numbers plays an increasingly large role in two issues currently plaguing American society. Identity theft victimizes thousands of Americans every year, and the number of identity theft crimes continues to grow. This crime begins, in many cases, with the misuse of a Social Security Number. And Homeland Security has become an even greater focus for all Americans. We have learned over the past 7 months that protecting a Social Security Number and preventing identity fraud is not only a criminal justice issue, but a Homeland Security challenge.

On behalf of the Inspector General, who could not be here today, I would like to touch briefly on each of these issues, starting with identity theft.

As you know, the Social Security Number was never intended to be a national identification number, but we can longer pretend otherwise. A vital part of commercial transactions of every kind, the SSN is as much a part of our identity as our own name. Indeed, the SSN is a more unique identifier—many people share common names, but an SSN is issued only once. For this reason, a valid SSN is an almost priceless tool for identity thieves. With an SSN in hand, unscrupulous individuals can apply for credit cards, open bank accounts, take out loans, apply for government benefits, obtain jobs, and do the many things all of us do every day, but these unscrupulous individuals do so fraudulently under an assumed identity.

In fiscal year 2000, more than half of the 92,000 allegations received by our fraud hotline were allegations of SSN misuse. The victims of identity crimes face situations similar to those described by the witnesses here today—feelings of violation and helplessness, and a long, difficult road to financial recovery. We have made some progress. Certainly the public is more aware of identity theft, and of the importance of protecting their SSN and other personal information than, they have ever been. And the Social Security Administration, which has adopted some of the recommendations made in our audit report, has taken important steps in tightening the process by which Social Security Numbers are issued and used.

On the investigative side, we see more and more indictments and convictions for identity theft crimes around the country. Right here in Florida, agents from my office, working with the Florida Department of Law Enforcement, brought the very first case indicted by Governor Bush's 16th statewide Grand Jury for the Purpose of Investigating Identity Theft, resulting in the indictment of six individuals with multiple counts of identity theft. Around the country, similar efforts have ensured that while identity theft may not be a difficult crime to commit, the prosecution of those who commit

identity theft is now more of a priority for law enforcement agencies.

As great a challenge as identity theft has become, the true severity of the larger SSN misuse problem became horribly apparent after the attack of September 11. We have come to learn in the 7‡ months since that day just how critical it is that we protect the integrity of the Social Security Number. We knew that our credit rating depended on it; we know now that our lives may depend on it.

There is no greater issue in the Homeland Security arena than protecting the integrity of the Social Security Number. It is virtually impossible to operate in the United States without a Social Security Number. It stands to reason, then, that any enemy of the United States that wants to infiltrate our borders and live among us would need a Social Security Number in order to do so. The challenge before us is to find a way to allow legitimate commerce to continue using the SSN for legitimate purposes while making it less simple for both identity thieves and even more dangerous individuals to misuse SSNs.

Part of that solution lies with SSA and its OIG. Many of the recommendations we have made to improve the enumeration process are already in place or in the process of being implemented. For example, SSA's practice of issuing "non-work" SSNs to visitors to our country so that they may obtain drivers licenses has been discontinued. Development of a meaningful process for SSA to verify immigration documents with the Immigration and Naturalization before issuing an SSN has been expedited. And SSA appreciates the need to do all it can under current law and within the position of budgetary constraints to protect the SSN upon its issuance during the life of the number-holder, and upon the number-holder's death.

In OIG, we have worked around the clock since September 11, both in support of the investigation into the events of that day, and in furtherance of Federal efforts to prevent future acts. An example is our participation in Operation Tarmac in 12 major airports around the country. The most recent of these was in the Washington, DC, area, where last week, together with other Federal authorities, we arrested some 105 individuals suspected of providing false information—including SSNs—to obtain work in secure areas of Reagan National Airport, Dulles International Airport, and Baltimore-Washington International Airport. Again, working within the limitation of existing laws—laws which were written for a time before identity theft and Homeland Security became the overarching issues they are today—we have taken significant steps.

But we need the help of this Subcommittee and the Congress as a whole. Legislations must be enacted to close the gaps in the laws that govern the use of SSNs. Legislation like H.R. 2036, the Social Security Number Privacy and Identity Theft Protection Act of 2001, introduced by this Subcommittee, places meaningful restrictions on the use, display and sale of SSNs and provides new and important enforcement mechanisms for offenders. Such legislation represents an important step to reducing identity theft and making the SSN unavailable as a tool to those who commit or support acts of terror against the United States.

The Inspector General looks forward to working with this Subcommittee to ensure that we are doing all we can to stem the tide of SSN misuse. Thank you.

[The prepared statement of Ms. Maye follows:]

Statement of Roland Maye, Special Agent-in-Charge, Atlanta Field Division, Office of the Inspector General, Social Security Administration, Atlanta, Georgia

Good morning, Chairman Shaw, and thank you for inviting the Office of the Inspector General (OIG), Social Security Administration (SSA), to testify today. My name is Roland Maye and I am the Special Agent-in-Charge of the criminal investigative activities in this region.

As you noted in your opening remarks, the misuse of Social Security numbers (SSNs) plays an increasingly large role in two issues currently plaguing American society. Identity theft victimizes thousands of Americans every year, and the number of Identity Theft crimes continues to grow. This crime begins, in many cases, with the misuse of an SSN. And Homeland Security has become an even greater focus for all Americans. We have learned over the past 7 months that protecting the SSN and preventing Identity fraud is not only a criminal justice issue, but a Homeland Security challenge. On behalf of the Inspector General, who could not be here today, I would like to touch briefly on each of these issues, starting with Identity Theft.

As you know, the SSN was never intended to be a national identification number, but we can no longer pretend otherwise. A vital part of commercial transactions of every kind, the SSN is as much a part of our identity as our own name. Indeed, the SSN is a more unique identifier—many people share common names, but an SSN is issued only once. For this reason, a valid SSN is an almost priceless tool for identity thieves. With an SSN in hand, unscrupulous individuals can apply for credit cards, open bank accounts, take out loans, apply for government benefits, obtain jobs, and do the many things all of us do every day.

In Fiscal Year 2000, more than half of the 92,000 allegations received by our fraud hotline were allegations of SSN misuse. The victims of Identity crimes face situations similar to those described by the witnesses here today—feelings of violation and helplessness, and a long, difficult road to financial recovery. We have made some progress. Certainly the public is more aware of Identity Theft, and of the importance of protecting their SSN and other personal information, than they have ever been. And SSA, which has adopted some of the recommendations made in our audit reports, has taken important steps in tightening the process by which SSNs are issued and used.

On the investigative side, we see more and more indictments and convictions for Identity Theft crimes around the country. Right here in Florida, agents from my office, working with the Florida Department of Law Enforcement, brought the very first case indicted by Governor Bush's 16th Statewide Grand Jury for the Purpose of Investigating Identity Theft, resulting in the indictment of six individuals with multiple counts of Identity Theft. Around the country, similar efforts have ensured that while Identity Theft may not be a difficult crime to commit, the prosecution of those who commit Identity Theft is now more of a priority for law enforcement agencies.

As great a challenge as Identity Theft has become, the true severity of the larger SSN misuse problem became horribly apparent after the attacks of September 11th. We have come to learn in the 7 months since that day just how critical it is that we protect the integrity of the SSN. We knew that our credit ratings depended on it; we know now that our lives may depend on it.

There is no greater issue in the Homeland Security arena than protecting the integrity of the SSN. It is virtually impossible to operate in the United States without an SSN. It stands to reason, then, that any enemy of the United States that wants to infiltrate our borders and live among us would need an SSN in order to do so. The challenge before us is to find a way to allow legitimate commerce to continue using the SSN for legitimate purposes, while making it less simple for both Identity Thieves and even more dangerous individuals to misuse SSNs.

Part of that solution lies with SSA and its OIG. Many of the recommendations we have made to improve the enumeration process are already in place or in the process of being implemented. For example, SSA's practice of issuing "non-work" SSNs to visitors to our country so that they can obtain drivers licenses has been discontinued. Development of a meaningful process for SSA to verify immigration documents with the Immigration and Naturalization Service before issuing an SSN

has been expedited. And SSA appreciates the need to do all it can under current law and within existing budgetary constraints to protect the SSN upon its issuance, during the life of the number-holder, and upon the number-holder's death.

In OIG, we have worked around the clock since September 11th, both in support of the investigation into the events of that day, and in furtherance of Federal efforts to prevent future acts. An example is our participation in Operation Tarmac in 12 major airports around the country. The most recent of these was in the Washington, DC area, where last week, together with other Federal authorities, we arrested some 105 individuals suspected of providing false information—including SSNs—to obtain work in secure areas of Reagan National Airport, Dulles International Airport, and Baltimore-Washington International Airport. Again, working within the limitations of existing laws—laws which were written for a time before Identity Theft and Homeland Security became the overarching issues they are today—we have taken significant steps.

But we need the help of this Subcommittee and the Congress as a whole. Legislation must be enacted to close the gaps in the laws that govern the use of SSNs. Legislation like H.R. 2036, The Social Security Number Privacy and Identity Theft Protection Act of 2001, introduced by this Subcommittee, places meaningful restrictions on the use, display, and sale of SSNs and provides new and important enforcement mechanisms for offenders. Such legislation represents an important step toward reducing Identity Theft and making the SSN unavailable as a tool to those who commit or support acts of terror against the United States.

The Inspector General looks forward to working with this Subcommittee to ensure that we are doing all we can to stem the tide of SSN misuse.

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

Chairman SHAW. Thank you. I would like to address this to anyone on the panel who has information, the question of repeat offenders.

Ms. GUIALDO. They are very common. It is every week the same person. It is a constant issue. Right now I have cases where a perpetrator used one person's name. We cleared that person's name. Well, he is also on two other person's cases.

Chairman SHAW. Has he been apprehended?

Ms. GUIALDO. We refiled charges against him, but the police department does not actively go out and pick you up. If he gets stopped using his own name, he will be apprehended for the new crimes. But if he is not, it doesn't happen.

Chairman SHAW. Is that the case up here, Sheriff? Are you talking about misdemeanors?

Ms. GUIALDO. Yes.

Mr. COHEN. Usually, they are misdemeanors. Usually just the plain using somebody else's name, unless it results in specified harm, it is a misdemeanor. If there is a certain harm——

Chairman SHAW. Well, if it is grand theft to—identity theft, yes, the felony, I mean the felony they will go get them, won't they?

Mr. COHEN. That is probably a statewide problem is basically the arrest on these warrants. I mean the police departments prioritize, you know, different degrees. They put different efforts into the fugitive squads of the different police departments. That is a constant resource issue, the apprehension of outstanding felons or outstanding fugitives.

Chairman SHAW. Sheriff?

Mr. BIELUCH. We probably have right now some 50 to 60,000 warrants just in our Palm Beach County database, and we don't actively go out after misdemeanants; however, perhaps we should in this case. I have made a note of it, and this obviously has the po-

tential to become a serious felony. As we said, stated over and over again, because nobody gets hurt, because it is not a crime against person, these things tend not to be investigated as thoroughly. And when the warrants come out, sometimes they probably don't go pick them up as quickly as they could. But I am going to take note of that, and we definitely will be going after the misdemeanor identity theft cases.

Chairman SHAW. We heard two felony cases today——

Mr. BIELUCH. Right.

Chairman SHAW. From our witnesses. Also, you are quite right as to what a growing problem it is. This is the fastest growing crime in the United States today. Still what we are looking at today is probably a drop in the bucket compared to what it is going to be, and unless we start getting some vigorous law enforcement and some arrest, it will go even faster.

Mr. BIELUCH. Yes, I agree. But, you know, all criminals have MOs, and this is just the MO of the people that do identity theft. And burglars get out of jail, and they don't suddenly become car thieves. They go back to being burglars because that is kind of their trade, and the punishment is nil.

Mr. COHEN. But it is not just a crime. It really—it is not just the crime, it is the means to a crime. It really is. And a lot of people say identity theft is a crime. I think that it really is—it is just part of your grand theft, it is part of your credit card fraud, it is part of your forgeries. And that is all it is, is a tool. Instead of pushing them down and grabbing their purse and then using their credit card, they are just applying in the mail for one.

Mr. FOLEY. Identity theft is the getaway car, just one issue. Sergeant Rispoli, I appreciate, and all of your testimony I appreciate specifically, but you did a nice job of outlining what are good areas for us to look into: education, enhanced penalty, the companies themselves—not a day goes by that I don't end up with something in my mailbox for a free teaser ad, get 1.5-percent interest rate for the next 30 hours, and then it goes to 19 percent.

Mr. RISPOLI. If you get to the mailbox first.

Mr. FOLEY. Right, exactly. And that is the problem. People are going into your mailbox and gaining some of this information. The web postings, these are all interesting suggestions.

Mr. Maye, as well, with the Social Security Administration, thank you for illuminating some of the problems we are facing relative to immigration. It is a whole other—I talked to a person the other day, because I asked—I know their status is illegal, I asked, "How you are able to work here?" They said, "Oh, five or six of us use the same person's Social Security Number." I said, "Five or six? Doesn't Social Security ever check how he has five or six jobs?" He said, "Oh, no. It has never happened to him yet." But I mean these things are going on, and so people are either using numbers collectively or gaining them illegally, and so it is a frightening aspect, because we all, again, feel very, very vulnerable.

Mr. MAYE. In some cases this is true, especially in the agricultural areas, the person employing the workers are the ones who don't do the necessary checks to ensure that each worker has a valid number. They are more concerned with gathering their crops, so they might look the other way. We have had several cases on

some major producers that hired individuals without valid SSNs because they didn't do the proper checks to ensure that each individual they hired had a valid SSN.

Mr. FOLEY. No, but it is interesting, and I fault government a lot, and whether we fail to live up to technology we have to look at the problem. I mean I can use an ATM card in Europe. I can put it in a machine, it reads my bank account in the United States, determines if I have a balance and in about 15 seconds it sends me back cash in the denomination of the country I am in. Now Social Security, you would think, if somebody was an employer, they could call up and verify within 15 seconds whether the person presenting themselves had a valid Social Security Number and maybe some outliers, like they ask my grandmother's maiden name. If there was an ability to do that, then I would shoulder the responsibility mostly on the employer community. But I don't know who they call today, and I don't know how long it would take.

Mr. MAYE. Social Security has such a system in place.

Mr. FOLEY. Is it?

Mr. MAYE. An employer can call and verify an SSN with SSA.

Mr. FOLEY. Quickly?

Mr. MAYE. Yes, expeditiously.

Mr. FOLEY. Well, then, God bless, we have gotten something going on, because that is a big concern.

Mr. MAYE. It is just a matter of getting employees oriented to contacting Social Security and verifying the employee's SSN.

Mr. FOLEY. Well, then we will work on that aspect of it. Because it was one of the concerns that I had that we didn't have enough means in which to determine. And then fraudulent documents are a problem as well for employers. There is a lot of things that go on. Thank you.

Chairman SHAW. I would like to thank you all. I think we always learn something from a field hearing, and this has been very helpful to us to see the frustrations of prosecution and law enforcement and trying to get these things done.

The bill that we have filed that we are working on would have penalties up to 5 years in jail for people that were trapped in these numbers. So the identity theft would become—would also become a felony, not just a misdemeanor under what we are proposing. So we still have some work to do, but we will look into it, and I think we will be able to use your experience in developing this legislation as we see it through. I am hopeful that we can get the bill passed in short order to get this thing moving. What happens over in the Senate, which is the graveyard of legislation, I have no idea, but we will do our part.

Thank you all for being here. Say hello to Mike for me. We go back 30-some years. Thank you.

[Whereupon, at 3:45 p.m., the hearing was adjourned.]

[Submissions for the record follow:]

Plantation, Florida 33322
May 10, 2002

The Honorable E. Clay Shaw, Jr.
Chair, Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives

Dear Representative Shaw, Chair, and Committee Members:

This letter is in reference to protecting the privacy of social security numbers and preventing identity theft. In coming across information regarding the already held Subcommittee Hearing in Lake Worth through the Congressional website, there was also details for submission of written comments by May 13, 2002. I am a concerned private citizen wishing to submit comments on this subject.

Increasingly, more articles are released by the media highlighting the pervasive misuse of social security numbers (SSNs) by criminals and terrorists. It is now known that a majority of the September 11th terrorists fraudulently obtained false SSNs to carry out their activities and this has exemplified the severe consequences of the failure to protect the integrity of SSNs. I commend Congress for taking steps to protect the privacy of every Americans' SSN and, as you have indicated, it is an appropriate action in the Nation's response to terrorism.

There appear to be many issues related to the fraudulent use of SSNs, ranging from law enforcement issues to the ease of accessibility to target victims with identity theft, on account of the widespread use of SSNs as an identification method by businesses, government, medical, and educational institutions. There is a strong need for preventative measures and legal protections to be put in place for U.S. citizens. Public and private entities routinely request the surrender of an individual's SSN as a course of business. As a result, it gets harder for an individual to control access to their own SSN leaving them exposed as victims to potential criminal activity. A serious concern of mine relates to the routine request for SSN by medical practices and health insurances. Not only do many health insurances have practices such as issuing cards announcing an individual's SSN to all parties but also many hospitals, doctors, and others in the medical industry make releasing a SSN a condition to receiving medical attention. Denial of business services due to refusing to submit SSN may currently be an option for those providing consumer goods and services but should not be permitted for medical and insurance providers for its potential serious repercussions and unfair access to medical care. All these industries may have a legitimate need for individual identifiers, including obtaining payment for services, products and insurance, but not by contributing to the exposure of SSNs to potential fraud and the peril of its customers. It is my hope that such concerns be addressed to reduce the common use of SSNs.

I would like to be kept informed on the progress of the legislation being considered. Thank you for your attention to the matter.

Sincerely,

Maisy Alpert

Statement of David Palay, Las Vegas, Nevada

I urge all members of the Committee to DISREGARD the complaints of industry about limitations on the use of Social Security Numbers and take steps to prohibit all use except for income tax purposes as originally intended and as promised by former President Roosevelt originally. Consider an unseen computer, selling personal information to anyone with the price of access. That is what the system has become. Is not one's name and identification personal property? Please make it so.

(Don't worry about placing the nuke repository at Yucca Mountain. Its the right place for these materials)

○