IDENTITY THEFT: ASSESSING THE PROBLEM AND EFFORTS TO COMBAT IT

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

DECEMBER 15, 2003

Serial No. 108–60

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

91–576PDF WASHINGTON : 2004

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

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
Vice Chairman
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California

DAN R. BROUILLETTE, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

JAMES C. GREENWOOD, Pennsylvania, *Chairman*

MICHAEL BILIRAKIS, Florida
CLIFF STEARNS, Florida
RICHARD BURR, North Carolina
CHARLES F. BASS, New Hampshire
GREG WALDEN, Oregon
Vice Chairman
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

PETER DEUTSCH, Florida
Ranking Member
DIANA DEGETTE, Colorado
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HENRY A. WAXMAN, California
BOBBY L. RUSH, Illinois
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

IDENTITY THEFT: ASSESSING THE PROBLEM AND EFFORTS TO COMBAT IT

MONDAY, DECEMBER 15, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Langhorne, PA.

The subcommittee met, pursuant to notice, at 10:12 a.m., in Middleton Township Municipal Building, Langhorne, Pennsylvania, Hon. James C. Greenwood (chairman) presiding.

Members present: Representatives Greenwood and Gerlach.

Staff present: Ann Washington, majority counsel and Billy Harvard, legislative clerk.

Mr. GREENWOOD. Good morning, everyone. I am Congressman Jim Greenwood, and I am chairman of the Subcommittee on Oversight and Investigations of the Energy and Commerce Committee, and I would like call this hearing to order.

We thank you all for being here. Welcome to this field hearing of the Subcommittee on Oversight and Investigations of the House Energy and Commerce Committee.

We are here today to discuss the problem of identity theft, one of the fastest growing white collar crimes in the United States. The Federal Trade Commission estimates that each year, 10 million Americans fall victim to identify theft, which translates into tremendous costs, both for the defrauded businesses and for the victimized consumers.

What I hear from victims time and again is how draining the experience is, both emotionally and financially. Luckily, most victims are protected so that they usually do not incur any actual out of pocket loss. The problem lies in the other ways in which the theft of Social Security numbers, bank account numbers and related financial and personal information affects an individual's life.

A victim's good credit can be severely damaged to the point of preventing the legitimate purchase of a new car or house, and the damage can take months to correct.

What is astounding is the audacity of these thieves. They steal bill payments from your mailbox, they make scamming phone calls to banks. We have all heard some of the stories, but let me highlight a few particularly egregious ones.

In 2001, a restaurant busboy in Brooklyn, New York used computers at a library, web-enabled cell phones, virtual voicemail and courier services to try to steal the identities of more than 200 CEOs, celebrities and tycoons. Their names were posted in a Forbes article on the 400 richest people in America. The crook was

caught when one of the transactions he attempted drew attention because of its size, a transfer of $10 million from an account owned by Thomas Siebel, founder of Siebel Systems.

In 2002, the largest ring of identity thieves was apprehended for stealing tens of thousands of credit reports over a period of 3 years. The ring members allegedly stole credit reports from three major commercial credit reporting agencies and used that information to siphon funds from bank accounts and to make fraudulent purchases. Authorities have accounted for $2.7 million in losses from that ring so far.

And just last month, a California man was arrested for stealing computers containing the personal information of thousands of Wells Fargo Bank customers. The man was apprehended at his home with the computer and equipment used for scanning identity cards and checks.

According to the FTC's Identity Theft Clearinghouse Data base, in Pennsylvania alone, 5,080 consumers reported that they were victims of identify theft in 2002. People between the ages of 30 and 39 were hardest hit. This is the time in life when typically people are starting to accumulate good credit and considering some of those important life decisions like buying a home or having a child, decisions that can be greatly complicated if one's credit has been damaged.

Today, we will hear testimony from several victims of identity theft, Michelle Kane, whom I had the pleasure of meeting recently, and State Representative Bernie O'Neill, who as a victim himself and how assists other victims with their plight.

We will hear from the Red Cross, which has also fallen victim to identity theft. This is a double travesty. The services that a reputable organization like the Red Cross provides, are essential to us all in times of great need. For someone to put an organization of the Red Cross' caliber at jeopardy by attempting to steal personal information from its blood donors is deplorable. I hope the Federal law enforcement agencies currently pursuing such actions will quickly find the perpetrators and swiftly bring them to justice.

We will also hear today testimony from representatives from the private sector organizations that have to contend with identity theft, Bob Ryan from TransUnion and Missy Lenahan from a local financial institution, First National Bank and Trust. Banks are on the front line of this type of fraud, fielding the initial calls from victims and taking most of the financial losses.

We will hear from Betsy Broder of the Federal Trade Commission, and Kevin Burke of the U.S. Postal Inspection Service this morning. They will discuss their efforts to assist victims and to chase down the fraudsters who so callously use other people's identities for their own purposes.

John Abel from the Pennsylvania Attorney General's Office and Lieutenant Colonel Ralph M. Periandi from the Pennsylvania State Police will testify about their offices' efforts to combat this problem here at home and what services they can offer to victims.

I want to thank everybody for participating this morning. We want to provide the public with as much assistive information as we can this morning as to what steps they can take to avoid becoming victims, and in the event that they do fall victim to this fraud,

what they can do to stop the financial bleeding as quickly as possible.

We recognize and are pleased that the Fair and Accurate Credit Transaction Act, or the FACT Act, was just signed into law by President Bush on December 4. This will provide victims of identity theft with additional assistance and protections by giving national uniformity to industry best practices regarding identity theft prevention and aid. I am eager to see the benefits flowing from this implementation of this Act, but also believe it is prudent to build a record on this important issue in this Subcommittee in case it becomes necessary to consider additional legislation within our Committee's jurisdiction on this topic further down the road.

So I thank all of the witnesses for being, and I would like to yield now to my Pennsylvania Congressman—colleague, Congressman Jim Gerlach, who while not a member of this Subcommittee, is an active participant in legislating on this issue. Mr. Gerlach, welcome to Bucks County, and the microphone is yours.

Mr. GERLACH. Thank you, Mr. Chairman, and thank you very much for the opportunity to be here today and to listen to the testimony of those that present to us on this very important issue.

In addition to the facts that you have set forth to give us a sort of broad opening view of this problem nationwide, I wanted to have an opportunity to submit some remarks for the record which we have here on the issue that I have been involved in since being contacted by the Montgomery County District Attorney, Bruce Castor, on this issue some time ago.

And what I would like to do is just maybe highlight some of those remarks very briefly, and hopefully allow that to also set a stage for what we are going to hear today from our presenters. In Montgomery County, hundreds of individuals were victimized by the owner of an auto dealership in Limerick Township. The victims provided their personal information to the alleged thief in their efforts to buy a new car. He then allegedly used that information to obtain more than $4 million in loans, some of which were fraudulent on their face and some which were legitimate loans used for fraudulent purposes. For instance, the thief secured the loans as requested by the victims, but instead of paying off the liens on the victims' old cars, used the money for his own purposes.

Civil and criminal cases were then brought in Montgomery County, and those are pending, as a result of that fraudulent conduct, and while these victims may eventually receive financial damages, they have found themselves in a quagmire when it comes to getting their credit record repaired. After receiving notification from the Montgomery County District Attorney that these loans were fraudulently obtained, many creditors refused to withdraw any negative notations or entries on the victims' credit record. Further, many of these victims continue to be harassed by creditors or collection agencies, and some face foreclosure on their belongings, loss of life savings, and an inability to get loans of any kind.

As many of the Montgomery County victims have found, while the thief may be criminally prosecuted, the burden to repair the damage inflicted by an identity thief is on the one that is harmed, and the only method by which one can individually attempt to repair his or her good name and credit is by pursuing civil action

against the creditors and debt collectors. This has proven very difficult, very time consuming and very expensive. That is why we have introduced legislation called PITFALL, Prevent Identity Theft From Affecting Lives and Livelihoods Act, which provides relief and alternatives to those who have already been victimized by an identity thief. While existing legislation primarily focuses on prevention or mitigation of the crime, this legislation is designed to aid those for whom prevention and mitigation is too late. When existing laws fail to protect identify theft victims, this legislation prevents creditors, debt collectors, consumer reporting agencies and financial institutions from harassing victims and further sabotaging their financial well-being.

Once the State's highest law enforcement officer, or in this case, a District Attorney of one of the counties of the Commonwealth of Pennsylvania, has conclusively determined that the debt or loan was fraudulently incurred, under the legislation, once the law enforcement official determines that a person is, in fact, a victim, a no fault statement would be issued. This statement would cite the victim's lack of involvement in obtaining the debt or loan, and the victim may then forward the statement to creditors, debt collectors, credit reporting agencies and financial institutions.

Upon receipt of the no fault statement, any business acting as a creditor, credit agency, or collector would be required to cease all collection activities and hold the victim harmless from any fraudulently incurred financial obligations. They would further be required to withdraw or correct any negative entries on the victim's credit history with regard to those transactions or obligations created by the identity theft.

Failure to recognize this no fault statement by those institutions and to cease collection activities or remove negative entries from the credit record would result in State enforcement and civil liability. It would also, the legislation, fill gaps in the law such as that which has allowed creditors to continue harassing the Montgomery County victims despite a determination by the law enforcement officials in that locality that they were not involved in incurring the debt.

This legislation makes enforcement provisions in the Truth in Lending Act, the Fair Credit Reporting Act, the Fair Debt Collections Practices Act and the Electronic Funds Transfer Act consistent. Each of these Acts currently provide for civil liability and administrative enforcement, and the Fair Credit Reporting Act also provides for State enforcement in Federal District Court, and the Electronic Funds Transfer Act provides for criminal liability. The Truth in Lending Act currently permits State enforcement, but only for predatory lending practices.

To make these four important Acts consistent, this legislation, H.R. 2396, will amend the Fair Debt Collection Practices Act and Electronic Funds Transfer Act to permit a State to bring about an action against a person or entity acting in violation of the PITFALL provisions. The PITFALL legislation will also expand State action provisions in Truth in Lending Act and provide actual damages, monetary fines and in the severest cases, imprisonment for violations.

So you can see that, given what is even happening in our local area, there is a lot of need for continued Federal oversight and legislative action on this issue, and I want to extend my appreciation for you for taking on this issue as chairman of the subcommittee, and look forward to all the important information and testimony we will receive today.

Thank you.

Mr. GREENWOOD. Thank you, Congressman Gerlach. Before we call our first witness, I thought it would be an interesting way to introduce this subject. We are going to present a video made by the Postal Inspection Services that outlines, rather dramatically, what the—how this crime takes place and what its consequences may be. Technical difficulties here. Is it rewound? Here we go.

[Video shown.]

Mr. GREENWOOD. Okay. Now playing the part of our first witness will be State Representative Bernie O'Neill, and Mr. O'Neill, will you please come forward.

Welcome, thanks for being with us this morning.

Mr. O'NEILL. Thank you.

Mr. GREENWOOD. You can have a seat. As you—and if you want to bring one of the black microphones in front of you. As you probably have been told, this is an investigative hearing, and when we——

Mr. O'NEILL. Sure.

Mr. GREENWOOD. [continuing] take testimony at an investigative hearing, we do it under oath. Do you have any objections to giving your testimony under oath?

Mr. O'NEILL. Not at all.

Mr. GREENWOOD. Okay. I also need to advise you you are entitled to counsel. This was something that was very important to our Enron witnesses, but probably not important to you. Do you wish to be advised by counsel?

Mr. O'NEILL. Not at all.

Mr. GREENWOOD. Okay. Then if you would stand and raise your right hand.

[Witnesses sworn.]

Mr. GREENWOOD. You are under oath and you are recognized for your statement, sir.

TESTIMONY OF HON. BERNARD T. O'NEILL, PENNSYLVANIA STATE REPRESENTATIVE; MICHELLE KANE; AND BRIGID O'NEILL-LAGIER, RED CROSS CHIEF EXECUTIVE OFFICER, AMERICAN RED CROSS BLOOD SERVICES

Mr. O'NEILL. Thank you, Mr. Chairman. Good morning. Good morning, Congressman Gerlach.

Mr. GREENWOOD. Probably want to bring the microphone even a little closer than that. There.

Mr. O'NEILL. How is that? Here? I am State Representative Bernie O'Neill, from the 29th Legislative District here in Central Bucks County, and with me today is my legislative aide, Cindy Beck, who is leading the education effort on identify theft here in Bucks County.

Identity thieves steal more than $1 billion a year from unsuspecting and unprepared consumers. In the bulk of cases, the

consumers don't know their identity theft—were stolen. Credit card fraud accounts—or excuse me, credit card fraud accounts for 42 percent of the complaints, followed by scams where phone and utility accounts were created in a person's name without his or her knowledge.

With these, criminals make thousands of dollars at their victim's expense. The victim is left with years of anguish and frustration trying to sort out and restore his good name and credit, or clear a criminal record.

I am here today to share with you how identity theft has grown, especially here in Bucks County, and what we are trying to do to stop it. While the other witnesses today will go into the staggering statistics and efforts being undertaken to combat identity theft, I am here to put a face on this appalling crime.

Anyone can become a target of identity theft. Thieves are stealing personal information from a number of different sources, including credit card receipts, birth certificates and Social Security cards. Just putting your bills in your mailbox to be sent out is a sign to a would-be identity thief that you are an easy target.

To educate my constituents about this growing crime, I am holding public forums on identity theft throughout my legislative district. These forums will continue through the month of February. These forums have been very well attended. Our first forum was in Solebury Township on November 14. We have had presentations by local law enforcement officials, including Chief Richard Mangan of Solebury Township Police Department, Chief Henry "Rick" Pasqualini of the New Hope Borough Police Department and representatives from the Pennsylvania's Attorney General Office and the United States Postal Inspection Service.

Dates are being finalized for the series of upcoming identity theft forums throughout the 29th Legislative District. January programs have been scheduled for Buckingham Township with Chief Daniels, Warminster Township with Chief Jim Gorczynski and a second evening forum in New Hope-Solebury with Chief Mangan and Pasqualini. February programs have been scheduled in Warwick Township with Chief Costello and Upper Southampton Township with Chief Schultz. Topics have included tips on avoiding identity theft, ways in which identity theft occurs and why students as well as senior citizens are targeted.

It is sad that victims do not become aware that their identities have been stolen until they get an astronomical credit card statements, cell phone bills and other charges.

I can personally attest that obtaining this information is far too easy. From my own personal experience, my phone number was stolen and for 3 to 4 months, my phone bill exceeded $300 to $500 in total charges. That number was used from the same pay phone in New York City, and my case is minor compared to other stories that have been shared with me. Even local enforcement officials who I have been dealing with have been victims of identity theft themselves.

As a State legislator, I have been involved in helping make identity theft less attractive to would-be thieves. Last year, a new law was enacted that escalates the penalties for this crime. Through legislation introduced by Representative Matt Baker of Wellsboro,

Tioga County, the Pennsylvania House of Representatives has taken steps to increase the penalties for identity theft, making a first offense of the crime a felony of the third degree, carrying a maximum penalty of 7 years in prison and a $15,000 fine. A third or subsequent offense raises the crime to a felony of the second degree, with a maximum penalty of 10 years in prison or a $25,000 fine.

I am hopeful these forums will help residents become more educated about identity theft and will learn how they can protect themselves and their identities. There is nothing more frustrating than finding out that your whole identity has been stolen and used for fraudulent purposes. And I can tell you since we began the forums, my wife and I have stopped putting our mail in our mailbox with the little red flag up, and we have purchased a shredder for our home. I have always used one in the office, but it never dawned on me of using one at home.

So, I am more than welcome to answer any questions that you may have.

[The prepared statement of Hon. Bernard T. O'Neill follows:]

PREPARED STATEMENT OF HON. BERNIE O'NEILL, REPRESENTATIVE, PENNSYLVANIA STATE HOUSE

Good morning. I am State Rep. Bernie O'Neill from the 29th Legislative District in central Bucks County.

Identity thieves steal more than $1 billion a year from unsuspecting and unprepared consumers. In the bulk of the cases, the consumers don't know how their identities were stolen. Credit card fraud accounts for 42 percent of the complaints, followed by scams where phone or utility accounts were created in a person's name without his or her knowledge.

While these criminals make thousands of dollars at their victim's expense, the victim is left with years of anguish and frustration trying to sort out and restore his good name and credit or clear a criminal record.

I'm here today to share with you how identity theft has grown, especially here in Bucks County and what we're trying to do to stop it. While the other witnesses today will go into the staggering statistics and efforts being undertaken to combat identity theft, I'm here to put a face on this appalling crime.

Anyone can become a target of identity theft. Thieves are stealing personal information from a number of different sources, including credit card receipts, birth certificates and Social Security cards. Just putting your bills in your mailbox to be sent out is a sign to a would-be identity thief that you are an easy target.

To educate my constituents about this growing crime, I am holding public forums on identity theft throughout my legislative district. These forums will continue through February.

These forums have been very well attended, with 50 to 60 people coming out for our first forum in Solebury on Nov. 14, 2003. We have had presentations by local law enforcement officials, including Chief Richard Mangan of Solebury Township Police Department, Chief Henry "Rick" Pasqualini of the New Hope Borough Police Department, and representatives from the Pennsylvania Attorney General's Office and the United States Postal Inspection Service.

Dates are being finalized for the series of upcoming identity theft forums throughout the 29th legislative district. January programs have been scheduled in Buckingham Township with Police Chief Stephen Daniels, Warminster Township with Police Chief Jim Gorczynski, and a second evening forum in New Hope-Solebury, with Chief Richard Mangan and Chief Henry "Rick" Pasqualini. February programs have been scheduled in Warwick Township with Police Chief Joe Costello, and Upper Southampton Township with Police Chief David Schultz.

Topics have included tips on avoiding identity theft, ways in which identity theft occurs, and why students as well as senior citizens are targeted.

It is sad that victims do not become aware their identities have been stolen until they get astronomical credit card statements, cell phone bills, or other charges.

I can personally attest that obtaining this information is far too easy. From personal experience, my phone number was stolen and for three months my phone bill

exceeded $300 in toll charges. That number was used from a pay phone in New York City. And my case is minor compared to other stories that have been shared with me. Even local law enforcement officials are identity theft victims.

As a state legislator, I have been involved in helping make identity theft less attractive to would-be thieves. Last year, a new law was enacted that escalates the penalties for this crime. Through legislation introduced by Rep. Matt Baker from Wellsboro, Tioga County, the Pennsylvania House of Representatives has taken steps to increase the penalties for identity theft, making a first offense of the crime a felony of the third degree, carrying a maximum penalty of seven years in prison and a $15,000 fine. A third or subsequent offense raises the crime to a felony of the second degree with a maximum penalty of 10 years in prison and a $25,000 fine.

I am hopeful these forums will help residents become more educated about identity theft and will learn how they can protect themselves and their identities. There's nothing more frustrating than finding out that your whole identity has been stolen and used for fraudulent purposes.

Mr. GREENWOOD. Thank you, Representative O'Neill. The Chair will recognize himself for questioning. Tell us about after you discovered that your telephone bill was inflated and calls were being made from a pay phone in New York City. Was it difficult for you to—what did you go through with the phone company so that they would accept the fact that these were not your obligations?

Mr. O'NEILL. Right. The first thing I did was I—when I got the first phone bill, which exceeded $300, I called the phone company and I explained to them that these weren't my charges and I didn't understand where they were coming from, and they said they would investigate it, and they actually sent me some paperwork to fill out.

It continued for several months after that, and they eventually were able to find out that what was actually stolen was my phone card ID number, which is very interesting, because I didn't carry the card with me. I never had the card. I knew it by rote memory, so what is really appalling is how they were able to get that number and use it.

Mr. GREENWOOD. Did you ever figure out how they did that?

Mr. O'NEILL. To this day, we have never figured out how they ever got the number. The number was subsequently canceled, and that is when the charges certainly stopped. I believe, if I am not mistaken, I was held accountable for $50 each month for those expenses, and I did receive a phone call from the phone company several months later telling me that they finally tracked that all the phone calls were—every one of them were made from the same pay phone in—somewhere in the city of New York.

Mr. GREENWOOD. And they were never able to catch the perpetrator?

Mr. O'NEILL. No, they never did catch him or her, no.

Mr. GREENWOOD. And of course, you were personally responsible for the $50.

Mr. O'NEILL. Yes.

Mr. GREENWOOD. The phone company picked up the rest. That means we all——

Mr. O'NEILL. Yes.

Mr. GREENWOOD. [continuing] picked up the rest.

Mr. O'NEILL. Everyone paid for it. That is correct.

Mr. GREENWOOD. And I think that is an interesting thing that we found, is that frequently, as I mentioned in my opening statement, the victim him or himself may have limited financial exposure, and the credit card companies frequently have limited expo-

sure, and it frequently falls to the—if it is a retail purchase, the retail store ends up absorbing the loss, which again means that in terms of the billions of dollars that are stolen in this method, that it is built into the prices that we all pay for goods and services.

One of the issues that the Congress wrestles with in general, but in this case specifically, is whether to act Federal legislation, given the fact that obviously, here in your case, it was a crime perpetrated—you could say it was perpetrated in New York, you could say it was perpetrated in Pennsylvania.

Mr. O'NEILL. Correct.

Mr. GREENWOOD. Or both. And the need for interstate cooperation is—and harmonization is important. On the other hand, some states, particularly California, which has a very strict law, doesn't like the fact that the U.S. Congress, most notably just on the bill signed by the President on December 4, superseded State law.

Now, you are a State legislator. Do you have a view on whether you think it is appropriate for the Congress to supersede State laws, or do you think the states need to have their own——

Mr. O'NEILL. Well, I would think—I think each State needs to certainly enact their own laws and make them as stiff as possible for what happens within the confines of their own state, but I would agree with you that I think the Congress has to—I can tell you that I am the guardian of my aunt, who is well along in Alzheimer's. And I am now dealing with her credit cards, which we are beginning to think they were fraudulently used, because we are talking about $28,000 were run up on her charge cards and not in this state, and we have no idea how these numbers ever got out, other than the fact that, you know, when she——

Mr. GREENWOOD. Is your credit card number, which was what was stolen from you, is that printed on your phone bill?

Mr. O'NEILL. No.

Mr. GREENWOOD. That doesn't show up on your phone bill.

Mr. O'NEILL. Not that I am aware of, no. No.

Mr. GREENWOOD. And certainly the PIN number does not.

Mr. O'NEILL. No.

Mr. GREENWOOD. So someone would have either——

Mr. O'NEILL. Yeah, I——

Mr. GREENWOOD. [continuing] I guess just hacked into the system to get your—to match your phone number——

Mr. O'NEILL. Somehow, I actually saw on—a couple years ago, I saw on—it was either 20/20 or one of those type of shows on television, ways that they were stealing numbers at airports and that sort of thing when you were using them, and that may have been how it was taken. We are not really sure.

Mr. GREENWOOD. And I suppose also someone could theoretically stand next to you at a phone and watch and listen as you——

Mr. O'NEILL. Well, that is basically what they do in an airport, in a busy airport. They sit there and—they make—pretend they are making a phone call, and they are standing right next to you and you are punching in your number and they are just watching your numbers go in, which is also your PIN number as well, after you——

Mr. GREENWOOD. Right.

Mr. O'NEILL. [continuing] punch in the number.

Mr. GREENWOOD. Thank you. Congressman Gerlach?

Mr. GERLACH. No questions, but the exact same thing happened to me.

Mr. O'NEILL. Oh, jeez.

Mr. GERLACH. With my long distance credit card number, phone number, and——

Mr. O'NEILL. Right.

Mr. GERLACH. [continuing] had about 2 months worth of couple hundred dollars charges, calls to Europe, which I know I——

Mr. O'NEILL. Yeah.

Mr. GERLACH. [continuing] wouldn't have made, and you know, the phone company resolved it, but the exact same situation as yours.

Mr. O'NEILL. Right.

Mr. GERLACH. And I had no idea how they got the numbers to do that, other than maybe, you know, the service plaza on the turnpike. I went back from Harrisburg at that time, and maybe somebody was standing next to me, but you know, you punch those numbers pretty darn quick.

Mr. O'NEILL. Yeah.

Mr. GERLACH. You wonder how they can even keep track of it, but it is a bad problem, so I know exactly what you mean. But thank you.

Mr. O'NEILL. Thank you.

Mr. GREENWOOD. Thank you. We have no further questions for you.

Mr. O'NEILL. Thank you.

Mr. GREENWOOD. We appreciate your appearance here this morning. Thank you.

Mr. O'NEILL. Have a good day.

Mr. GREENWOOD. And the Chair would now call forward our two next witnesses for the first panel, Mrs. Michael Kane of Warminster and Brigid O'Neill-LaGier, Chief Executive Officer of the American Red Cross Blood Services for the Penn-Jersey Region.

Welcome. And I think we need you to make sure you pull those—each pull your microphone quite close to you as you testify, because they are apparently very directional. As—welcome and thank you again for being here this morning, both of you.

As you heard me indicate to Mr. O'Neill, we take our testimony under oath in this Committee. Do either of you have any objections to giving your testimony under oath?

Ms. O'NEILL-LAGIER. No.

Mrs. KANE. No.

Mr. GREENWOOD. Okay. And you are both represented—entitled to be represented by counsel. Do either of you wish to be represented by counsel this morning?

Ms. O'NEILL-LAGIER. No.

Mrs. KANE. No need.

Mr. GREENWOOD. Okay. If you would stand, then, and raise your right hands.

[Witnesses sworn.]

Mr. GREENWOOD. You are under oath, and I think we will start alphabetically with Mrs. Kane. Welcome, and——

Mrs. KANE. Good morning. How are you?

Mr. GREENWOOD. I am very well. How are you?

Mrs. KANE. Nervous.

Mr. GREENWOOD. Nervous. No need to be nervous. And you have as much time as you would like to make a statement for us this morning.

Mrs. KANE. Okay. Can you hear me? No? Okay.

Mr. GREENWOOD. All right. Tap on your—on that—okay. We have some ability to control the volume of the microphone. It seems to be on, but not——

Mrs. KANE. Okay. Is that better?

Mr. GREENWOOD. Can you hear in the back yet?

TESTIMONY OF MICHELLE KANE

Mrs. KANE. All right. Identity theft has been referred to as an invisible assault, and I should know, because unbeknownst to me, a woman from Schenectady, New York was able to steal my good name.

A little over 2 years ago, I was offered a free credit report. My credit was perfect, and I was expecting to receive a report that reflected that. Imagine my surprise when my report history came back 33 pages thick. I assumed there must be some sort of mistake of the credit agencies. Perhaps my name was mingled with another Michelle Kane. I had heard of that happening. After all, I had always been very careful with the use of my credit cards and my Social Security number. Boy, was I wrong.

Unfortunately, the credit agencies were not mistaken. A woman from Schenectady, New York had been using my Social Security number for approximately 2 years, and managed to charge over $70,000 in my name. She started out small, opening a few credit cards, and then gained more confidence, obtaining a car loan and eventually a mortgage.

The perpetrator, who is also named Michelle Kane, said she received the Social Security number from a friend and just thought she was able to use it. However, investigators believed that she obtained it through her place of employment. She worked for a vision company and had access to insurance company data bases. The Schenectady, New York Michelle Kane did get caught and served a year in prison, thank to the fact that investigators hired by the mortgage company worked so diligently.

Even though the woman went to jail, the task of clearing my credit history still existed. The red tape and jumping through hoops started from the very beginning. The first step of reporting the crime was not very simple. I first called the Schenectady Police Department, and they were unable to do anything because I could not file a report in person. It was 5 hours away.

When I called my local police department and they were unable to do much, because it was not in their jurisdiction. It did not get much easier with the three credit agencies, TransUnion, Experian and Equifax. They did send the information to me in my credit reports, but it was up to me to decipher it. The agencies' listed the creditors. However, many times as an abbreviation, and the biggest hassle was getting a phone number to go along with the bank. Sometimes, it was listed and sometimes, it was not. To get a number that was a 1-800 number that corresponded to the correct de-

partment in the bank was a rarity. For example, my husband and I spent countless hours trying to contact one of the names that was on the list, which was Verizon NE. It sounds simple enough until you try and actually find them. No one in the company knew who Verizon NE was when you called Verizon. Was it Northeast, New England, Nebraska? Which division did Verizon—which division of Verizon were we trying to contact? A wireless line, a land line, the Internet? So the countless hours of trying to figure out who you are contacting was very hassle-some.

Aside from the financial burden of huge phone bills and trying to track down the banks, and the countless hours wasted trying to sort through the red tape, the biggest problem is proving your identity to the creditors and convincing them that you did not make the charges. Over 2 years have passed, and I am hopeful that my credit history will soon be clear. I am hopeful that this does not come back to haunt me, and I am hopeful that there will be some improvements for the rest of the victims out there.

Now, I was told if I wanted to make some suggestions, which I did.

[The prepared statement of Michelle Kane follows:]

PREPARED STATEMENT OF MICHELLE KANE

Identity Theft has been referred to as the "invisible assault", and I should know because unbeknownst to me, a woman was able to steal my good name.

A little over two years ago, I was offered a free credit report. My credit was perfect and I was expecting to receive a report that reflected that. Imagine my surprise when my report history came back 33 pages thick.

I assumed there must be some sort of mistake with the credit agencies. Perhaps my name was mingled with another Michelle Kane; I have heard of that happening. After all, I have always been very careful with the use of my credit cards and Social Security Number. Boy, was I wrong!

Unfortunately, the credit agencies were not mistaken. A woman from Schenectady, New York had been using my Social Security Number fro approximately two years and had managed to charge over $70,000 in my name. She stated out small, opening a few credit cards, then gained more confidence obtaining a car loan and eventually a mortgage.

The perpetrator, who is also named Michelle Kane, said she received the Social Security Number from a friend and thought she was able to use it. However, investigators believe she obtained it through her place of employment. She worked for a vision company and had access to insurance company databases. The Schenectady, New York Michelle Kane did get caught and served a year in prison thanks to the fact investigators hired by the mortgage company work so diligently.

Even though this woman went to jail, the task of clearing my credit history still existed. The red tape and the jumping though hoops started from the very beginning. The first step of reporting the crime was not very simple. I first called the Schenectady Police Department and they were unable to do anything unless I filed a police report in person. I then called my local police department they were unable to do much because it was not in their jurisdiction.

It did not get any easier with the three credit agencies (Transunion, Experian and Equifax). They sent the information, but it was up to me to decipher it. The agencies listed the creditors, however many times just as an abbreviation. One of the biggest hassles was getting a phone number to the bank. Sometimes it was listed and sometimes it was not. To get a phone number that was a 1-800 number that corresponded to the correct department in the bank was a rarity. *I.e.,* My husband and I spent countless hours trying to contact Verizon NE. No one in the company knew who this was; did NE stand for North East, New England, Nebraska? Which division of Verizon was this; wireless, landline or Internet?

Aside from the financial burden of huge phone bills trying to track down the banks, and the countless hours wasted trying to sort though the red tape, the biggest problem is proving your identity to the creditors and convincing them you didn't make the charges.

Over two years have passed and I am hopeful that my credit history will soon be cleared. I am hopeful that this does not come back to haunt me. And I am hopeful that there will be improvements for the rest of the victims out there.

My Suggestions for Improvement:

- Free yearly credit reports
- Transunion, Experian and Equifax list a local advocates phone number on the credit report. (Consumer Protection Number).
- Mandatory listing of all creditors' phone numbers that appears on credit report. (1-800).

Mr. GREENWOOD. Go ahead.

Mrs. KANE. Okay. My first suggestion is that there be some sort of legislation, which I know there are some people working on this for a free credit report from the credit agency, whether it be via email or, you know, it is expensive to send postage to thousands and thousands of people, but I think in the long run, it could save lots of money.

TransUnion, Experian and Equifax, I think should list a local advocate, a phone number on their credit report, which I was just going blindly through this, and I think it would save a lot of hassle if maybe at the end of the credit report, they say you can contact your local consumer report person and here is the steps which you follow, so you just don't go blindly through this.

And last, a mandatory listing of all of the creditors' phone numbers that appear on your credit report, so you don't have to, once again, track down these people and try and clear your credit. They don't even give you, for security purposes, your account number. So when you are trying to tell them who you are, the first thing they say is your account number, please, and you don't have it, so.

Anyway, they are my suggestions, oh, and, of course, a 1-800 number at which to contact them, so.

Mr. GREENWOOD. Those are very good suggestions, and that is why we are holding this hearing, to learn things like that. Thank you.

Mrs. KANE. You are welcome.

Mr. GREENWOOD. Ms. O'Neill-LaGier, am I pronouncing that right?

Ms. O'NEILL-LAGIER. Yes, you are.

Mr. GREENWOOD. Okay.

Ms. O'NEILL-LAGIER. Thank you.

Mr. GREENWOOD. Make sure you speak directly into the microphone, please.

Ms. O'NEILL-LAGIER. I will try to do that.

Mr. GREENWOOD. You are recognized for your testimony.

TESTIMONY OF BRIGID O'NEILL-LAGIER

Ms. O'NEILL-LAGIER. Good morning, Mr. Chairman, and Congressman Gerlach. Thank you for your invitation to testify on the important subject of identity theft.

I am Brigid O'Neill-LaGier, Chief Executive Officer of the Penn-Jersey Blood Services Region of the American Red Cross, headquartered in Philadelphia. I would respectfully ask that my entire statement and attachments be included in the record.

Mr. GREENWOOD. And will be without objection.

Ms. O'NEILL-LAGIER. The Red Cross has been helping people since 1881. You can see us at work in communities across the coun-

try and here in southeastern Pennsylvania and New Jersey, thousands of times a day, teaching first aid or CPR classes, keeping members of the military and their families connected through emergency communications, caring for disaster victims, and collecting and delivering blood.

Thousands of area residents participate in that work as volunteers, blood donors and financial contributors. As one of 36 Red Cross regional blood services, the Penn-Jersey region is the major supplier of blood in southeastern Pennsylvania and New Jersey.

Continuing a tradition begun more than 50 years ago, the mission of the Penn-Jersey region is to fulfill the community's need for the safest, most reliable and cost-effective blood products and transfusion services.

In 1994, the Red Cross dedicated the Musser Blood Center, which houses the blood supply for more than 125 southeastern Pennsylvania and New Jersey hospitals; the Philadelphia National Testing Laboratory, which provides infectious disease and type testing of blood donations for 4 Red Cross blood centers and several non-Red Cross blood centers; and the National Reference Laboratory for Blood Group Serology, serving more than 3,000 hospitals nationwide.

Hospitals and patients in southeastern Pennsylvania and New Jersey benefit from an array of transfusion support services including lifesaving blood products delivered 24 hours a day, 365 days a year, and physicians and technical experts available for consultation around the clock.

Mr. Chairman, last year, the Penn-Jersey Region collected more than 262,000 whole blood donations and nearly 11,000 platelet and granulocyte donations, and additionally imported 135,000 blood products to meet the local community transfusion needs of over 800,000 blood products.

In southeastern Pennsylvania and New Jersey, the Red Cross conducted over 11,000 blood drive operations, which assisted over 300,000 volunteer blood donors who stepped forward to save lives. The Red Cross takes the confidentiality of our blood donors very seriously. As a regulated service, blood collection is a very detailed process designed to ensure the safety and security of the blood donor, the blood supply and those who are trained to collect, manufacture and distribute blood products.

The Food and Drug Administration Center for Biologics Evaluation and Research is responsible for regulatory oversight of the U.S. blood supply. FDA promulgates and enforces standards for blood collection and for the manufacturing of blood products, including both transfusable components of whole blood, pharmaceuticals derived from blood cells or plasma, and related medical devices. The American Red Cross Penn-Jersey Blood Region activity is regulated not only by the FDA, but also, on a local level, by the State of Pennsylvania, the State of New Jersey, AABB, as well as national American Red Cross standards, policies and procedures.

As you may know, an investigation is currently being conducted by Federal authorities into identity theft at the American Red Cross Penn-Jersey Blood Region. Investigators learned that several individuals' personal identification information, such as names and Social Security numbers, had been used to obtain credit and make

purchases. A common denominator was that they had all donated at one of four Red Cross blood drives held in the southeastern Pennsylvania area in November and December 2002.

We have recently learned that several donors at two additional blood drives during the same period were victims of identity theft. Social Security numbers are utilized during the donation process to uniquely identify each blood donor and help us accurately connect the donor with his or her donation history, which is important for both donor and patient safety. While advances in technology and record keeping have afforded us increased security options, Social Security numbers remain the universally accepted means of identification.

Upon learning of the problem in February 2003, we immediately contacted the U.S. Attorney's Office for the Eastern District of Pennsylvania and requested that an investigation be opened and a task force of Federal law enforcement officials be developed to fully investigate the matter. We are also working closely with the Federal Bureau of Investigation and the U.S. Postal Inspection Service. We have acted aggressively and cooperated fully with investigators to assist them in resolving this matter quickly and thoroughly. We have also launched a rigorous review of our security procedures. We have no reason to believe that our electronic data base has been compromised. This continues to be an open case, and consequently, I am sharing with you only the details that have been made public and will not hinder the ongoing investigation. We want to make clear that the safety of the blood supply has in no way been compromised.

To date, the investigation has been contained in the southeastern Pennsylvania area, and limited to six blood drives in the November through December 2002 timeframe. We are aware of at least 23 individuals who were blood donors and were also victims of identity theft. Our first concern is for those who may have been victimized. I have personally contacted representatives of the four blood drive sponsor groups, and I am in the process of contacting the two new groups we learned about last week. We have notified 1,400 donors in writing who participated in the first four blood drives, and letters are going out to all donors from the two additional identified blood drives. I have attached a generic copy of that correspondence for the record. This letter gives step by step actions they should take if they are concerned about the security of their personal information. The information was provided to us by Federal law enforcement officials.

In addition to the information in the letter, we have set up a special Red Cross toll-free telephone number to assist donors who believe they may have been victims. This line is answered by specially trained staff to provide more detailed information about security of donor information and to assist donors in checking their credit reports.

Despite this isolated situation, you can be certain that specific steps are taken throughout the Penn-Jersey Region's blood donor centers to ensure that blood donor information is secure. Some of them include that donor records are handled exclusively by authorized personnel trained to deal with confidential information. Before interacting with the public, our blood service region employees go

through in-depth training that also requires signing a confidentiality agreement and a Code of Conduct agreement.

Information entered on the blood donation record form completed by donors at the blood drive is protected from view by others during the donation process, and access to information is limited to authorized staff who need it in order to process the blood donation.

Every person who handles this information is known and identified to us. Also, once donor information is entered into a computer at the blood center, the blood donation record form is shredded, and access to our computers and computer data bases is strictly limited.

Mr. Chairman, the Red Cross relies on voluntary donations to ensure a safe and adequate blood supply. We regret that any donor has had to question his or her desire to give blood because of security concerns. We are committed to ensuring the safety and privacy of our donors and are working diligently to ensure that this situation is not repeated. We are appreciative of the thousands of donors who continue to support us every day. Without their generous donation of the gift of life, lives would be lost.

Finally, we are proud of our people and the job they do. We hope that the details surrounding this case will not discourage people from donating blood in the future. Increasing the available supply of blood is critical to health care in our community, because much of modern medicine is only made possible because of blood donations. Yet, donations do not always keep pace with demand.

Philadelphia is a major regional medical center with teaching hospitals that provide advanced care, such as organ transplants, specialized pediatric and neonatal care, cancer and cardiac care, all of which require a stable blood supply.

For our region, blood donations given locally only meet 70 percent of our true need. Through planning and coordination, the Red Cross is able to ship blood from communities where there is an excess to those where there is a need. Still, history shows that our reserves of blood are not—have not been strong enough to compensate for seasonal swings in donations and weather-related disruptions of normal blood collection activities. Additionally, blood shortages seriously affect patient care. As the population ages, the need for blood is predicted to grow.

Experts agree that a stronger blood supply is an essential part of community preparedness. After the terrorist attacks of September 11, 2001, a multidisciplinary task force of representatives from government agencies and the blood banking community was formed to study this issue. The task force concluded that the single biggest determinant of the success of the blood community's first response to a disaster, is the blood already on the shelves of blood centers and hospitals. It recommended that planning for future disasters include the requirement that all blood centers have available a 7-day supply of all blood types at all times.

To meet our responsibility to the people we serve, the Penn-Jersey Region will continue to increase our blood supply by asking more people to donate blood, asking those already giving blood to donate more often and asking business and community groups to increase their support.

On behalf of the Red Cross, thank you again, Chairman Greenwood, for the opportunity to testify before this Subcommittee. It is

imperative for our national preparedness and the daily treatment of those with life-threatening conditions that Americans generously donate blood. This act can and does save lives. I would be happy to respond to your questions.

[The prepared statement of Brigid O'Neill-LaGier follows:]

PREPARED STATEMENT OF BRIGID O'NEILL LAGIER, CHIEF EXECUTIVE OFFICER, PENN-JERSEY BLOOD SERVICES REGION, AMERICAN RED CROSS

Good morning, Mr. Chairman, Congresswoman Hart and Congressman Gerlach. Thank you for your invitation to testify on the important subject of identity theft. I am Brigid O'Neill LaGier, Chief Executive Officer of the Penn Jersey Blood Services Region of the American Red Cross headquartered in Philadelphia.

The Red Cross has been helping people since 1881. You can see us at work in communities across the country, and here in southeastern Pennsylvania and New Jersey, thousands of times a day—teaching first aid or CPR classes, keeping members of the military and their families connected through emergency communications, caring for disaster victims, and collecting and delivering blood. Thousands of area residents participate in that work as volunteers, blood donors and financial contributors.

As one of 36 Red Cross regional blood services, the Penn-Jersey Region is the major supplier of blood in southeastern Pennsylvania and New Jersey.

Continuing a tradition begun more than 50 years ago, the mission of the Penn-Jersey Region is to fulfill the community's need for the safest, most reliable and cost-effective blood products and transfusion support services. In 1994, the Red Cross dedicated the Musser Blood Center, which houses:

- The blood supply for more than 125 southeastern Pennsylvania and New Jersey hospitals;
- The Philadelphia National Testing Laboratory, which provides infectious disease and type-testing of blood donations for four Red Cross blood centers and several non-Red Cross blood centers; and
- The National Reference Laboratory for Blood Group Serology, serving more than 3,000 hospitals nationwide.

Hospitals and patients in southeastern Pennsylvania and New Jersey benefit from an array of transfusion support services, including:

- Lifesaving blood products delivered 24 hours a day, 365 days a year, and physicians and technical experts available for consultation around the clock;
- Products to meet special patient needs such as Granulocytes (infection fighting white cells) and HLA-matched platelets;
- Self-donation for planned surgery;
- Perioperative autologous cell salvage—a transfusion option benefiting orthopedic and other surgical patients;
- Reference laboratory services that identify and locate compatible units of platelets and red cells for patients;
- The American Rare Donor Registry—a joint American Association of Blood Banks (AABB) and Red Cross program that assists patients who need rare blood across the country and world;
- Stem cell and therapeutic apheresis services to help patients with cancer and other diseases;
- National Marrow Donor Program participation that helps cancer and other patients through donor recruitment and education; and
- Research activities in support of—
  - Cellular therapies to help cancer patients;
  - Pathogen inactivation techniques that may prevent the transmission of AIDS, hepatitis or bacterial contamination; and
  - Preservation and storage techniques for donated blood platelets so patients will receive the optimal benefit from their transfusion.

Mr. Chairman, last year the Penn-Jersey Region collected more than 262,000 whole blood donations and nearly 11,000 platelet and Granulocyte donations and additionally imported 135,000 blood products to meet the local community transfusion needs of over 800,000 blood products. In southeastern Pennsylvania and New Jersey, the Red Cross conducted over 11,000 blood drive operations, which assisted over 300,000 volunteer blood donors who stepped forward to save lives. The Red Cross takes the confidentiality of our blood donors very seriously. As a regulated service, blood collection is a very detailed process designed to ensure the safety and security

of the blood donor, the blood supply, and those who are trained to collect, manufacture and distribute blood products.

The Food and Drug Administration (FDA)'s Center for Biologics Evaluation and Research (CBER) is responsible for regulatory oversight of the U.S. blood supply. FDA promulgates and enforces standards for blood collection and for the manufacturing of blood products, including both transfusable components of whole blood, pharmaceuticals derived from blood cells or plasma, and related medical devices. The American Red Cross, Penn-Jersey Blood Region activity is regulated not only by the FDA, but also on a local level by the State of Pennsylvania, the State of New Jersey, AABB as well as national American Red Cross standards, policies and procedures.

As you may know, an investigation is currently being conducted by federal authorities into identity theft at the American Red Cross, Penn-Jersey Blood Region. Investigators learned that several individual's personal identification information, such as names and social security numbers, had been used to obtain credit and make purchases. A common denominator was that they had all donated at one of four Red Cross blood drives held in the southeastern Pennsylvania area in November and December 2002. We have recently learned that several donors at two additional blood drives during the same period were victims of identity theft.

Social security numbers are utilized during the donation process to uniquely identify each blood donor and help us accurately connect the donor with his or her donation history, which is important for both donor and patient safety. While advances in technology and record keeping have afforded us increased security options, social security numbers remain the universally accepted means of identification.

Upon learning of the problem in February 2003, we immediately contacted the U.S. Attorney's Office for the Eastern District of Pennsylvania, and requested that an investigation be opened and a task force of federal law enforcement officials be developed to fully investigate the matter. We are also working closely with the Federal Bureau of Investigation and the U.S. Postal Inspection Service. We have acted aggressively and cooperated fully with investigators to assist them in resolving this matter quickly and thoroughly. We also launched a rigorous review of our security procedures. We have no reason to believe that our electronic database has been compromised. This continues to be an open case and, consequently, I am sharing with you only the details that have been made public and will not hinder the ongoing investigation. We want to make clear that the safety of the blood supply has in no way been compromised.

To date, the investigation has been contained to the southeastern Pennsylvania area and limited to six blood drives in the November through December 2002 timeframe. We are aware of at least 23 individuals who were blood donors and were also victims of identity theft. Our first concern is for those who may have been victimized. I have personally contacted representatives of four blood drive sponsor groups and I am in the process of contacting the two new groups we learned about last week. We have notified 1,400 donors in writing who participated in the first four blood drives and letters are going out to all donors from the two additionally identified blood drives. I have attached a generic copy of that correspondence for the record. This letter gives step by step actions they should take if they are concerned about the security of their personal information. The information was provided to us by federal law enforcement officials.

In addition to the information in the letter, we have set up a special Red Cross toll-free telephone number to assist donors who believe they may have been victims. This line is answered by specially-trained staff to provide more detailed information about security of donor information and to assist donors in checking their credit reports.

Despite this isolated situation, you can be certain that specific steps are taken throughout the Penn-Jersey Region's blood donor centers to ensure that blood donor information is secure. Some of them include:

- Donor records are handled exclusively by authorized personnel trained to deal with confidential information. Before interacting with the public, our Blood Services Region employees go through in-depth training that also requires signing a confidentiality agreement and a Code of Conduct agreement.
- Information entered on the blood donation record form completed by donors at the blood drive is protected from view by others during the donation process.
- Access to information is limited to authorized staff who need it in order to process the blood donation.
- Every person who handles this information is known/identified to us.
- Once donor information is entered into a computer at the blood center, the blood donation record form is shredded.
- Access to our computers and computer databases is strictly limited.

Mr. Chairman, the Red Cross relies on voluntary donations to ensure a safe and adequate blood supply. We regret that any donor has had to question his or her desire to give blood because of security concerns. We are committed to ensuring the safety and privacy of our donors and are working diligently to ensure that this situation is not repeated. We are appreciative of the thousands of donors who continue to support us everyday. Without their generous donation of the gift of life, lives would be lost. Finally, we are proud of our people, and the job they do. We hope that the details surrounding this case will not discourage people from donating in the future.

Increasing the available supply of blood is critical to healthcare in our community, because much of modern medicine is only made possible because of blood donations. Yet, donations do not always keep pace with demand.

Philadelphia is a major regional medical center with teaching hospitals that provide advanced care, such as organ transplants, specialized pediatric and neonatal care, cancer and cardiac are, all of which require a stable blood supply.

For our region, blood donations given locally only meet 70 percent of our true need. Through planning and coordination, the Red Cross is able to ship blood from communities where there is an excess to those where there is a need. Still, history shows that our reserves of blood have not been strong enough to compensate for seasonal swings in donations and weather-related disruptions of normal blood collection activities. Additionally, blood shortages seriously affect patient care. As the population ages, the need for blood is predicted to grow.

Experts agree that a stronger blood supply is an essential part of community preparedness. After the terrorist attacks of September 11, 2001, a multi-disciplinary task force of representatives from government agencies and the blood banking community was formed to study this issue. The task force concluded that the single biggest determinant of the success of the blood community's first response to a disaster is the blood already on the shelves of blood centers and hospitals. It recommended that planning for future disasters include the requirement that all blood centers have available a seven-day supply of all blood types at all times.

To meet our responsibility to the people we serve, the Penn-Jersey Region will continue to increase our blood supply by asking more people to donate blood, asking those already giving blood to donate more often, and asking business and community groups to increase their support.

On behalf of the Red Cross, thank you again, Chairman Greenwood, for the opportunity to testify before this subcommittee. It is imperative for our national preparedness, and the daily treatment of those with life-threatening conditions, that Americans generously donate blood. This act can, and does, save lives. I would be happy to respond to your questions.

Mr. GREENWOOD. Thank you very much. Thank you for your testimony, and we are very sensitive to the fact that, as you said, the supply of blood in this area, blood products, is a life and death matter, and we hope that it is helpful to let people know in this region that the precautions that you have taken now to fully their secure their personal identity and that that will encourage more donation and not less, because it is a matter of life and death.

Let me recognize myself for some questions, and start with Mrs. Kane. Did the other Mrs. Kane, the bad Mrs. Kane.

Mrs. KANE. The evil one, yes.

Mr. GREENWOOD. The evil one. Went to jail for a year, you said. Did she serve that entire year, do you know, or——

Mrs. KANE. Yes. She was supposed to get 2 to 7 originally, but she served about a year.

Mr. GREENWOOD. She served about 1 year of a 2 to 7, but it might have been a 2 to 7 year sentence.

Mrs. KANE. Right. Well, she——

Mr. GREENWOOD. Do you know if she was ever required to make financial compensation to—either to yourself or to any of the businesses that were defrauded by her?

Mrs. KANE. I have no idea if she was required to do that. I don't know.

Mr. GREENWOOD. You didn't attend her trial or sentencing, or——

Mrs. KANE. I wasn't even notified until after she was sent to prison.

Mr. GREENWOOD. Well, that is interesting in and of itself, isn't it, that you were the victim and you weren't notified of what—you weren't kept abreast of what was going on with her prosecution.

Mrs. KANE. It was mostly the banks that were the victim, not me. So the banks knew about it and I found out after the fact.

Mr. GREENWOOD. Now, you indicated in your testimony that your—this happened—this—you discovered this how long ago?

Mrs. KANE. A little over 2 years ago.

Mr. GREENWOOD. A little over 2 years ago. And you are still not finished cleaning up your mess.

Mrs. KANE. We are about 95 percent.

Mr. GREENWOOD. Okay. What remains to be done?

Mrs. KANE. We just received the latest with our lovely Verizon. But we just received the third credit report of the three, and now they just have to take the 90 days or 30 to 90 days to make certain everything does come off. So hopefully, we are down to the last stretch.

Mr. GREENWOOD. All right. And it is interesting you said that the banks were the victims, not you. I mean, one of the things that we are trying to make clear here is yes, the banks were holding the financial bag as a result of this, but you and your husband obviously were victimized, because of the——

Mrs. KANE. Well, I certainly think so.

Mr. GREENWOOD. Right. Because—have you ever estimated how many hours of your time this has consumed?

Mrs. KANE. Countless.

Mr. GREENWOOD. Countless hours of your time.

Mrs. KANE. Countless. I have——

Mr. GREENWOOD. And you have had some phone bills, obviously, because you didn't have 800 numbers.

Mrs. KANE. The phone bills were a lot, and just the nitty-gritty daily grind of having to get the $8 credit reports again and again and again, and the notarized—every time you had to send a bank a notarized statement that this was not you, the $10 charge or whatever the nominal fee is, but it adds up.

Mr. GREENWOOD. And were there periods of time where you couldn't use your own credit, your own credit cards and so forth to——

Mrs. KANE. No, I was never——

Mr. GREENWOOD. That was not disrupted. Okay. Let me see what else I was going to ask you. What would you say was the best resource for you in trying to get this identity theft problem taken care of? Who was most helpful to you?

Mrs. KANE. It wasn't until I staggered through that I found out, through my own relatives, or people that I knew that had gone through this, which way to go. My one relative worked for the Social Security office and said, oh, make certain you check Social Security, or my neighbor was a police officer that said oh, make certain you do this. But it was not from the banks, it was not from the credit agencies. It was networking and a little bit of luck that

we found our way through it, and I hopefully don't find out more. We just 2 years after the fact, I figured out that there was a credit protection agency that could have helped me through this. I wish I would have known at the beginning.

Mr. GREENWOOD. Well, that gives me an opportunity to segue into the fact that for anyone in the room, there are materials at the front desk here that give some information about how to protect against—how to avoid identity theft, and also how to respond to it should it happen to you.

Let me ask a question or two of the representative from the Red Cross. You said that the Penn-Jersey Regional operation office has changed significantly, and you illustrated some of the ways that you changed your practices so that your staff is trained to protect identities, that only select people are able to view the identifying information for donated blood.

Do you know if those practices have been put into place in the Red Cross' activities throughout—in other regions of the country as well?

Ms. O'NEILL-LAGIER. Well, just to clarify, Mr. Chairman, those processes were in place prior to us knowing of the identity theft, so that is our standard practice.

Mr. GREENWOOD. Okay. It is—would—did you make changes—did you find that there were changes you had to make as a result or this, or not?

Ms. O'NEILL-LAGIER. We did a thorough review of our security, and there were very few changes that we made. There were a few things that we thought we could tighten up, but for the most part, we felt that our system was very secure.

Mr. GREENWOOD. Are you able to speculate, and we want to be sensitive to the fact that there is an ongoing investigation, and so you are perfectly free to say that you can't answer any of the questions, but have you been able to identify yet whether this was an inside job, so to speak, someone who worked for Red Cross, or whether it was someone who got access to this information who was not part of your organization?

Ms. O'NEILL-LAGIER. I would respectfully have to decline answering that.

Mr. GREENWOOD. Okay.

Ms. O'NEILL-LAGIER. As it is part of the investigation.

Mr. GREENWOOD. I understand that a person's Social Security number is still considered as—you mentioned in your testimony, the universally accepted means of ID, but in light of these recent events, has the Red Cross considered using other tracking methods besides the Social Security number?

Ms. O'NEILL-LAGIER. And that I can answer——

Mr. GREENWOOD. Okay.

Mr. O'NEILL-LAGIER. [continuing] with a positive yes. We are currently—the Red Cross, the entire organization, is currently producing a new donor card, which will have a unique donor identification number, and the new card will replace the Social Security number as the primary donor identifier, and will eliminate the need for the donor to verbally communicate their Social Security number at the blood drive. So, we expect that this initial distribution will begin in March 2004, and we expect to be fully imple-

mented in the Red Cross system by the summer. So, we are very——

Mr. GREENWOOD. And that would be nationwide?

Ms. O'NEILL-LAGIER. Yes.

Mr. GREENWOOD. Okay.

Ms. O'NEILL-LAGIER. For the Red Cross.

Mr. GREENWOOD. That is very good. So therefore, if somebody needs access to that, knows the numerals, there is nothing——

Ms. O'NEILL-LAGIER. Right. It will be——

Mr. GREENWOOD. [continuing] they could do with them to——

Ms. O'NEILL-LAGIER. [continuing] just unique to their blood donation——

Mr. GREENWOOD. Okay.

Ms. O'NEILL-LAGIER. [continuing] history.

Mr. GREENWOOD. The FDA oversees our Nation's blood supply, and the Red Cross is therefore subject to its regulations. Are there steps that the FDA should be taking to assist in protecting the blood donors and their personal information, because obviously, the Red Cross isn't the outfit involved in the blood supply.

Ms. O'NEILL-LAGIER. Well, the FDA requires that we are always able to track the blood donation back to the blood donor, and that is for many safety and security reasons, so we have to have a mechanism in place to always be able to take that donation back to the donor. An example of something that might require us to look back and be able to identify that donor is if a subsequent—a positive test on that donor would come up. We have to be able to go back to all of that donor's donations and recall them from the inventory, so it is critically important.

That is the requirement of the FDA, so when we moved to this unique Red Cross identifier, that will allow us to do that in the same way that the Social Security does.

Mr. GREENWOOD. But to your knowledge, the FDA hasn't come up with a regulatory scheme that says that all of the Nation's blood supplies should use these kind of non-Social Security identifying numbers.

Ms. O'NEILL-LAGIER. Not to my knowledge.

Mr. GREENWOOD. Okay. The FTC is tasked with being the flagship Federal Government agency for monitoring identity theft and providing guidance to victims. Did the Red Cross contact the FTC when this first happened?

Ms. O'NEILL-LAGIER. Well, we worked with the U.S. Attorney's Office, the FBI and the Postal Inspector Office, and they took care of any of that notification. We took their advice on the information to send out to the blood donors, which I have included, giving them some guidance on how to contact the credit agencies and to put fraud alerts on the credit reports.

Mr. GREENWOOD. Well, I think both of these cases illustrate the depravity of people who would take these numbers with total disregard to the impacts, in one case, very personal impact within a family and in another case, an impact, a series of impacts that could really be life and death matters, in terms of keeping a secure supply of blood.

The Chair recognizes Mr. Gerlach for questions.

Mr. GERLACH. Thank you. Just as a follow-up to that last comment. What has been the anecdotal feedback from those that have been identity theft victims that come through the blood drives that you have narrowed down as to be those that—potentially, was where the fraudulent activity generated from. What has been the anecdotal feedback as to what they have experienced after being victimized that way?

Ms. O'NEILL-LAGIER. Well, the victims that we—the Red Cross have talked to, you know, are very upset, very concerned. And very concerned that this would happen to the American Red Cross, because we truly have been victimized also. There has been a variety of amounts of money that were stolen. This is anecdotal to me. I mean, you could check with the investigators for better information, but it is really quite devastating to them and to us, because we just feel terrible about it.

Remarkably, many people have returned to donate again, and feel that it is their obligation as members of the community and are willing to work through this, and we have shared with the victims our intent to move away from Social Security number, and so they are willing to wait for us to get that in place.

Mr. GERLACH. Okay. And Mrs. Kane, on your—in your situation, the person that stole your identity was also named Michelle Kane, and do you know whether or not she, in fact, used other Michelle Kanes around the country, in addition to yourself as being the basis for which she undertook that fraudulent activity?

Mrs. KANE. I don't know if she found any other Michelle Kanes in her medical data base that she was able to find their Social Security numbers as well. All I know is my account.

Mr. GERLACH. Okay. When did you find out her identity as being the person that stole your identity? When in relation to the criminal prosecution she underwent and was convicted of and thereafter served time, when did you learn of her identity, so that you knew that was the person that stole your identity?

Mrs. KANE. When she applied for a mortgage and took out a $40,000 loan, that is when it became big enough for the banks to get involved, and the bank that was involved hired an investigator.

Mr. GERLACH. Okay.

Mrs. KANE. And it was through the investigator, he asked me did I wear glasses, which I thought was an odd question, because I only wore them for college, and I rarely wore them. I think I have worn them 10 times total, and at first, I said no, because it was so long ago, and then I said well, I do have a pair, and here, she worked for a vision company, and she was able to go through the medical data bases. According to the investigator, she denies that this is how it came to be, but—so it was once the mortgage company got involved that they told me how they think it went down.

Mr. GERLACH. And that information was passed along to law enforcement where she resided?

Mrs. KANE. Yes. They were——

Mr. GERLACH. And that was where?

Mrs. KANE. Schenectady, New York.

Mr. GERLACH. Schenectady. And then you had no contact yourself, however, with the Schenectady Police Department or the prosecuting attorney in that county——

Mrs. KANE. No.

Mr. GERLACH. [continuing] where Schenectady is located.

Mrs. KANE. No, I did not. I had only had contact with the investigator, who kept me abreast of the information.

Mr. GERLACH. Okay. And after these activities occurred, was anybody coming to you, either credit reporting agencies, with information? Obviously, you saw that it was inappropriate, but were any debt collectors or anybody coming, financial institutions coming after you for payment on loans or indebtedness that had been incurred in your name?

Mrs. KANE. Up until—once we got in touch with the credit agencies and once we told them we were victims, our number must have gotten onto the credit reports. Obviously, our phone number, our address, and then the debt collectors started calling us, but not beforehand, because she had her own Post Office box set up.

Mr. GERLACH. Okay.

Mrs. KANE. So once we got in the system, you would think the credit agencies would help. Instead, they put us down as—they—just mistaken. It was a mistake of which Michelle Kane they should call, and they started calling us to pay off these debts.

Mr. GERLACH. And what was your experience with those debt collectors?

Mrs. KANE. Well, it was not pleasant.

Mr. GERLACH. Did they accept your explanation that you were a victim?

Mrs. KANE. No, they just denied—they said, I am sorry, we don't believe you. You know, pay up, honey.

Mr. GERLACH. Okay.

Mrs. KANE. So.

Mr. GERLACH. And how long did that—how many different collectors were after you in that fashion?

Mrs. KANE. Well, it was——

Mr. GERLACH. And how long did it take them to realize that——

Mrs. KANE. It wasn't very long. It was only two banks, and it did eventually get cleared up, but it was still not something I was expecting.

Mr. GERLACH. Okay. And upon what information, if you know, did they rely upon to understand that you were a victim in this situation, and therefore should not be harassed with dunning notes or telephone calls? Did they receive information from some other source, either law enforcement in Schenectady or the private investigator hired by the one bank? Do you know how it was that they finally let you off the hook in terms of their thought that you should be paying on the debt?

Mrs. KANE. I think, and this is just my own personal thoughts, I don't think that they got any information from any other outside sources. I think they just probably did their homework and looked at the information that was in front of them and realized——

Mr. GERLACH. That you were telling the truth.

Mrs. KANE. That we were telling the truth.

Mr. GERLACH. Yeah.

Mrs. KANE. By looking at their information that we had sent through our credit—our criminal record. What did we send? The police reports and the ID and the notarized forms that they prob-

ably just put two and two together once we persisted enough and said that this is not us. But it took a few phone calls.

Mr. GERLACH. Okay. Thank you.

Mr. GREENWOOD. Thank you. One more question for Ms. O'Neill-LaGier. Are blood collection activities subject to the Act that protects the privacy of health information, HIPAA?

Ms. O'NEILL-LAGIER. The HIPAA. We are not obligated to HIPAA, but I would have to check on that for you and get back to you on that.

Mr. GREENWOOD. Okay. Would you do that and——

Ms. O'NEILL-LAGIER. Yeah. I will do that.

Mr. GREENWOOD. [continuing] communicate with the committee staff on that. Okay. We thank you both for being here and for your testimony and for your willingness to help us in our investigation, and you are both excused.

Mrs. KANE. Thank you.

Ms. O'NEILL-LAGIER. Thank you.

Mr. GREENWOOD. For the rest of the day. And we will now call forward the second panel, consisting of Mr. Robert Ryan from—he is the Senior Director of Government Relations for TransUnion, which is out of Chicago; and also Milissa Lenahan, who is the Assistant Vice President and Assistant Operations Officer for First National Bank and Trust, nearby in Newtown, Pennsylvania. Welcome, both of you.

Mr. RYAN. Thank you.

Ms. LENAHAN. Thank you.

Mr. GREENWOOD. You may sit down. Then I will ask you to stand up. As you have heard me say to the other witnesses that we take testimony here under oath, and so I need to ask if either of you objects to taking—giving your testimony under oath.

Mr. RYAN. No.

Mr. GREENWOOD. Okay. And you are both entitled to be represented by counsel. Do either of you choose to be represented by counsel?

Ms. LENAHAN. No.

Mr. RYAN. No, Mr. Chairman.

Mr. GREENWOOD. Okay. Now, if you would stand up again and raise your right hands.

[Witnesses sworn.]

Mr. GREENWOOD. Okay. You are both under oath, and I am going to start with you, Mr. Ryan. You are recognized to give your testimony.

TESTIMONY OF ROBERT RYAN, SENIOR DIRECTOR OF GOVERNMENT RELATIONS, TRANSUNION; AND MILISSA J. LENAHAN, ASSISTANT VP/ASSISTANT OPERATIONS OFFICER, FIRST NATIONAL BANK AND TRUST COMPANY OF NEWTOWN

Mr. RYAN. Good morning, Mr. Chairman Greenwood, Congressman Gerlach. My name is Bob Ryan, and I am the Senior Director of Government Relations for TransUnion. We are a leading global provider of consumer report information supported by more than 4,100 employees in more than 24 countries worldwide. I appreciate the opportunity to appear before you here today to discuss the role of TransUnion in the credit granting process, and in assisting con-

sumers, and our business customers in preventing and remediating identity theft.

I would like to explain briefly how TransUnion plays a critical role in the economic engine of credit availability. We provide the information necessary to lenders, regardless of where they are located, to make credit available to consumers all across the United States. In order for a lender to extend a loan to a consumer, the lender needs to evaluate the credit risks inherent in lending to that consumer, and the proper evaluation of the consumer's credit risks allows the lender to determine whether to provide credit to the consumer and at what price.

We believe that the most accurate and predictive piece of information a lender can use in evaluating credit risk is a consumer report, also commonly called a credit report, and we take great pride in our ability to collect and disseminate credit report information. We receive and process approximately 2 billion updates to consumers' credit files each month.

Now, let me turn to our role in thwarting identity theft. Identify theft is a serious problem and TransUnion is part of the solution. Since the 1980's, when TransUnion developed the first application fraud detection services for credit grantors, we have been helping our business customers detect and avoid application fraud, thus reducing the number of consumers affected by identity theft. In the mid-1980's, we were the first consumer reporting agency to initiate the development of special procedures to assist identity theft victims, including expedited dispute verification processes. In the late 1980's, we developed the innovation of a security alert flag on credit reports, to alert our customers to use extra caution in opening new accounts in the cases of prospective victims or actual victims of identity theft.

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

Our identify fraud specialists work with consumers, industry and government agencies to remediate damaged credit files as quickly as possible, to take preventative steps that reduce further victimization and to cooperate with law enforcement authorities in their investigations and prosecutions of this crime. Our processes include posting a security alert to the victim's file, opting the victim out of prescreened, pre-approved offers of credit or insurance, if he or she wishes, providing the victim a free credit report and notifying credit grantors and others, whose inquiries on the victim's file are due to fraud.

Congress, as you noted, Mr. Chairman, is also taking important steps with respect to identity theft. We applaud Congress for enacting the Fair and Accurate Credit Transactions Act, or the FACT Act, which makes permanent important national standards in the

credit reporting system and includes a comprehensive set of provisions pertaining to identity theft.

A significant provision of the new law is a requirement to provide a free credit report annually to consumers upon their request, so that was item one on Ms. Kane's suggestions. For many years, we have provided free credit reports to victims, and to individuals who think they may be—there may be fraudulent information on their reports.

The new law also provides for three types of security alerts in credit reports: an initial alert, for cases of potential fraud; an extended alert, in cases of actual identity theft; and a special active duty alert for our men and women serving in the armed forces stationed away from home.

TransUnion was a pioneer in giving consumers the opportunity to place security alerts in their credit files, as I noted a moment ago. The FACT Act also codifies what has been our industry's voluntary practice concerning the immediate blocking of information related to identity theft upon the consumer's providing us with an identity theft report. The FACT Act will also benefit consumers by requiring the Federal Trade Commission to develop a summary of consumer rights with respect to the procedures for remedying the effects of fraud or identity theft. The FACT Act also requires the consumer reporting agency to provide a heads-up, a notice, to a credit grantor if the grantor submits to a consumer reporting agency an address for a consumer that doesn't match an address in the consumer reporting agency's files.

At TransUnion, we are proud of our leadership in the development of processes and procedures to prevent and remediate identity theft. We applaud the 108th Congress for enacting the FACT Act, creating important, new national standards to help remediate identity theft, and we are gratified that many of the provisions of the bill were based on credit reporting industry standards that TransUnion helped to put in place.

Mr. Chairman, Congressman Gerlach, I sincerely appreciate your invitation to testify today on identity theft. TransUnion looks forward to continuing to be part of the solution to this terrible crime, and I would be pleased to answer any questions that you may have.

[The prepared statement of Robert Ryan follows:]

PREPARED STATEMENT OF ROBERT RYAN, SENIOR DIRECTOR OF GOVERNMENT RELATIONS, TRANSUNION

INTRODUCTION

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

THE ROLE OF TRANSUNION IN THE CREDIT GRANTING PROCESS

Consumer spending makes up approximately two-thirds of the U.S. gross domestic product. A critical component of this economic driver is the availability of consumer credit. Consumers in the United States have access to a wide variety of credit from a number of sources at extremely competitive prices. Consumers rely on the avail-

ability of credit for a variety of purposes, such as the purchase of homes, cars, education, and daily needs. In fact, there is approximately $7 trillion in outstanding mortgages and other consumer loans in the United States. There is no question that our economy would suffer if consumers could not easily access credit as they do today.

It is my pleasure to explain how TransUnion plays a critical role in the economic engine of credit availability. In sum, we provide the information necessary for lenders, regardless of where they are located, to make credit available to consumers all across the United States. In order for a lender to extend a loan to a consumer, the lender must evaluate the credit risks inherent in lending to that consumer. The proper evaluation of the consumer's credit risks allows the lender to determine whether to provide credit to the consumer and at what price. We believe that the most accurate and predictive piece of information a lender can use in evaluating a consumer's credit risk is a consumer report (also commonly called a credit report). TransUnion is in the business of providing lenders with this critical information.

The Credit Reporting Process

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

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

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

THE ROLE OF TRANSUNION IN IDENTITY THEFT PREVENTION AND REMEDIATION

TransUnion Is Part of the Solution

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

In 1992, we were the first national consumer reporting agency to establish a special Fraud Victim Assistance group within our organization that is solely dedicated to identity theft problems. In the 1997 we began immediate suppression, at the

same time the dispute investigation process was initiated, of fraud-related information on a consumer's file upon their presentation of a police report or other documentation confirming the fraud. In March 2000, this process became an industry standard.

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

THE IMPORTANCE OF NATIONAL STANDARDS IN COMBATING IDENTITY THEFT: THE FACT ACT OF 2003

The Fair and Accurate Credit Transactions Act of 2003

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

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

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

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

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

The FACT Act also requires a consumer reporting agency to provide a "heads up" to a user of credit reports if the user submits to a consumer reporting agency an address for a consumer that does not match an address in the consumer reporting agency's files. This provision is based on existing practices used by TransUnion to notify creditors and others that the consumer's address does not match one we have on file. This serves as another protection against identity theft, where the criminal may use a victim's identification information but the criminal's address in order to

obtain credit or other goods or services. Under the FACT Act, the user of a credit report that contains such a notice of discrepancy will need to take certain steps to reduce the risk that the transaction is the result of identity theft.

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

Furnisher Obligations

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

Reinvestigation Timeframes

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

CONCLUSION

At TransUnion, we are proud of our leadership in the development of processes and procedures to prevent and remediate identity theft. We applaud the 108th Congress for enacting the FACT Act, creating important new national standards that will help remediate identity theft. We are gratified that many of the provisions in the bill were based on credit reporting industry standards that TransUnion helped put in place.

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

Mr. GREENWOOD. Thank you very much, Mr. Ryan. Ms. Lenahan.

TESTIMONY OF MILISSA LENAHAN

Ms. LENAHAN. Hi. Thank you for the opportunity, and I would like to recognize American Bankers Association for giving me the opportunity to speak and they provided some materials, including a video, and I would just like for the record to recognize that.

Mr. GREENWOOD. Okay.

Ms. LENAHAN. My name is Milissa Lenahan. I have been employed by First National Bank and Trust Company of Newtown for 20 years. My current position is Assistant Vice President and As-

sistant Operations Officer, Security Officer and Custodian of Records.

Mr. GREENWOOD. Can you hear all right in the back, then? Okay.

Ms. LENAHAN. Okay. One of my primary functions as a Security Officer is researching and responding to fraud. I am currently working 20 cases of fraud that involve some form of identity theft. Twenty cases may not seem like a large number. However, First National Bank is a community bank, with our service area being in central and lower Bucks County. To us, one fraud is too many.

Identify theft is on the rise and no one is exempt from the possibilities of having their identity compromised. Identity theft takes several forms, from a stolen piece of mail to a wealth of counterfeit documents with unknowing victims' information.

My definition of identity theft is any time a person's information is used by someone other than themself. You don't have to have a fake driver's license to impersonate somebody and purchase something online with their stolen credit card. It has been my experience that retail locations rarely check the signature on the back of a credit card.

Our bank takes pride in its customer service and we will use our abilities and resources to assist our customers who have victimized by identity theft. We provide whatever assistance is necessary to stop any further damage to our customer's good name.

The following is a summary of the steps we take. Once notified by the customer, a hold is placed on all accounts. Notification is then broadcasted to every computer within the bank, tellers as well as back offices, as an alert. It is our practice to close customers' accounts and open new ones to prevent any future loss. We work with the customer in making sure legitimate payments are honored. We assist our customers with the paperwork necessary to credit back any missing funds as a result of the fraud, and in addition, we provide the customer with information on each credit reporting agency with the appropriate phone numbers, so that they can have an alert placed on their credit report.

We recommend that our customers file a police report, and we will cooperate with police in an attempt to catch the fraudster and bring them to justice. Training and education is a large part of what we do. It is an ongoing process and we will pool any and all resources available to us that is put out by organizations such as the American Bankers Association. We will use these resources in training, as well as provide them to our customers in their monthly statement. We post security alerts on our website as another type of warning to our customers, and we will speak to organizations and schools when asked.

The tellers on the front line are the most vulnerable to a perpetrator of identity theft. Split deposit fraud is one of the more common ways to pass yourself off as a customer by using a counterfeit or stolen check, presenting a portion for deposit and receiving a larger portion in cash back. The fraudster is usually prepared to present identification. The problem is there is no way for the teller to know that this identification is legitimate or not.

Our new accounts people are also at risk. Technology has broadened the spectrum for someone intent on committing fraud. The only equipment you need is a home computer and a printer. A fake

ID on the street would cost maybe $50. Check stock is readily available at stores that sell office supplies. All you need now is to take information off of someone's check. That check alone is a wealth of information, name, address, phone number, bank name, bank routing number and account number.

When I started my career in banking in 1983, the only way you could get a supply of checks was by submitting your order to your bank. A bank would have the tools necessary to determine if this order is fraudulent, as would the check printing company they contracted their business with. Unfortunately, resources necessary are not always available or practical. We no sooner put tools and policies into place and then you are hit with a fraud with a new twist.

Prevention is the key, but how do you prevent someone from stealing? If you are lucky enough to get an arrest, what is the punishment? Credit for time served and restitution that could take years. Our bank has a very good working relationship with local police departments, but police also have limited resources and tools to pursue these types of criminals. When our customer needs to file a police report, it is not clear which department they need to file with. Do you file in the municipality you live, or do you have a file in each location that an item was negotiated? One example of this that I had recently was our customer had to file a report in three separate municipalities after being turned away by their home municipality.

The consumer is depending on the police to help. Identity theft leaves consumers with the feeling of total personal violation regardless of the dollar amount. The consumer spends countless hours trying to repair the damage. That is why we depend on organizations such as the ABA, the FBI, the FTC and local law enforcement to communicate and provide new tools to assist us in educating not only ourselves but our customers as well.

Identity theft is one form of fraud that is extremely hard to prevent without access to certain tools only available to law enforcement. We can't call the police every time someone presents us with a driver's license to verify the validity of the document and the picture to the person in front of the teller. New technology is being made available in some states for this type of verification. Unfortunately, not in all states.

New regulations and policies, such as the PATRIOT Act and the Customer Identification Program will help in the prevention of new account identity theft, but for how long? If the people responsible for the crime are not punished for their actions, regardless of the dollar amount, it is only a matter of time before a new type of fraud surfaces. Government organizations, law enforcement, financial institutions and consumers all need to work together to stop this growing fraud.

Thank you.

[The prepared statement of Milissa Lenahan follows:]

PREPARED STATEMENT OF MILISSA J. LENAHAN, FIRST NATIONAL BANK AND TRUST

My name is Milissa J. Lenahan, I have been employed by The First National Bank and Trust Company of Newtown for 20 years. My current position is Assistant Vice President, Assistant Operations Officer, Security Officer and Custodian of Records. One of my primary functions as a Security Officer is researching and responding to fraud. I am currently working 20 cases of fraud that involve some form

of Identity Theft. 20 cases may not seem like a large number however, First National Bank is a Community Bank with our service area being within Central and Lower Bucks County. To us one fraud is too many.

Identity Theft is on the rise and no one is exempt from the possibilities of having their identity compromised. Identity Theft takes several forms from a stolen piece of mail to a wealth of counterfeit documents with unknowing victims information. My definition of Identity Theft is any time a persons information is used by someone other than them self. You don't have to have a fake Drivers License to impersonate someone and purchase something online with their stolen credit card. It has been my experience that retail locations rarely check the signature on the back of a credit card. Our bank takes pride in it customer service and we will use our abilities and resources to assist our customers who have been victimized by Identity Theft. We provide what ever assistance is necessary to stop any further damage to our customers good name. The following is a summary of the steps we take: Once notified by the customer, a hold is placed on all accounts. Notification is broadcasted to every computer, tellers as well as back offices as an alert throughout the bank. It is our practice to close the customers account and open new to prevent any further loss. We work with the customer in making sure legitimate payments are honored. We assist our customers with the paperwork necessary to credit back any funds missing as a result of the fraud. In addition we provide the customer with information on each credit reporting agency with the appropriate phone numbers so that they can have an alert placed on their credit report. We recommend that the customer file a police report. We will cooperate with police in an attempt to catch the "Fraudster" and bring them to justice.

Training and education is a large part of what we do. It is an on going process and we will pull any and all resources available to us that is put out by organizations such as American Bankers Association. We will use these resources in training as well as providing them to our customers in their monthly statement. We post security alerts on our web site as another type of warming to our customers, and will speak to organizations and schools when asked.

The tellers on the front line are the most vulnerable to a perpetrator of Identity Theft, split deposit fraud is one of the more common ways to pass yourself off as a customer by using a counterfeit or stolen check and presenting a portion for deposit and receiving a larger portion in cash back.

The "Fraudster" is usually prepared to present identification. The problem is there is no way for the teller to know if this identification is legitimate or not.

Our new accounts people are also at risk. Technology has broadened the spectrum for someone intent on committing fraud. The only equipment you need is a home computer and a printer.

A fake ID on the street would cost maybe $50.00. Check stock is readily available at stores that sell office supplies. All you need now is to take information off of someone's check. That check alone is a wealth of information, name, address, phone number, bank name, bank routing number and account number. When I started my career in banking in 1983, the only way you could get a supply of checks was by submitting your order to your bank. A bank would have the tools necessary to determine if this order is fraudulent as would the check printing company they contracted their business with.

Unfortunately resources necessary are not always available or practical. We no sooner put new tools and policies in place and then you are hit with a fraud with a new twist. Prevention is the key, but how do you prevent someone from stealing? If you are lucky enough to get an arrest, what is the punishment, credit for time served and restitution that could take years?

Our bank has a very good working relationship with local Police departments. But Police also have limited resources and tools to pursue these types of criminals. When our customer needs to file a Police Report it is not clear which department they need to file with. Do you file in the municipality you live in or do you have to file in each location that an item was negotiated.

One example of this I had recently was our customer had to file a report in three separate municipalities after being turned away by his home municipality. The consumer is depending on the Police to help. Identity Theft leaves consumers with the feeling of total personal violation regardless of the dollar amount. The consumer spends countless hours trying to repair the damage. That is why we depend on organizations such as the ABA, FBI, FTC and local Law Enforcement to communicate and provide new tools to assist us in educating not only ourselves but consumer as well.

Identity Theft is one form of fraud that is extremely hard to prevent without access to certain tools only available to Law Enforcement. We can't call the Police every time someone presents us with a drivers license to verify the validity of the

document and the picture to the person in front of the teller. New technology is being made available in some States for this type of verification, unfortunately not in all States.

New regulations and policies such as the Patriot Act and Customer Identification Program will help in the prevention of new account Identity Theft but for how long? If the people responsible for the crime are not punished for their actions regardless of the dollar amount, it is only a matter of time before a new type of fraud surfaces.

Government, Organizations, Law Enforcement, Financial Institutions and Consumers all need to work together to stop this growing fraud trend.

Mr. GREENWOOD. Thank you very much. The Chair recognizes himself for questioning. And we will start with you, Mr. Ryan.

You have heard the stories, including from Ms. Kane particularly this morning, that victims of identity theft find that the portion of their recovery that takes the longest is getting the fraudulent information off the victim's credit bureau. Can you explain what part of the process can take—why this part of the process can take such a long time, and what if anything is being done to shorten the time? Because I think Ms. Kane said that she was still trying to get—and one of the things she was—and I am a little bit confused, because you talked about free reports, and she said it was annoying to her to have to keep paying the $8 for the credit report. Was she not aware—do you think that she could get these for free?

Mr. RYAN. I can't—I can only speak, Mr. Chairman, for TransUnion, and to identity theft victims——

Mr. GREENWOOD. She mentioned TransUnion by name, I think, in her testimony.

Mr. RYAN. Our policy is to provide free disclosures to identity theft victims and has been for years, so I——

Mr. GREENWOOD. Well, let me—let us pursue that. If I am a victim of identity theft, and I say to myself, I better get my credit report, how would I—ordinarily, if I just go about the normal process of seeking a copy of my credit report, I would pay a fee unless—how would I know that I could get it for free?

Mr. RYAN. Well, no, that is part of our script—part of the VRU, part of our—both our 1-800 telephone toll-free number that is provided to consumers for calling in for your credit disclosure, for your credit report, and part of our Internet website disclosure is that under certain circumstances, you can be entitled—you are—may be entitled to a free disclosure. Obviously, in the case of any adverse action, under the Fair Credit Reporting Act, but also under Fair Credit Reporting Act and our longstanding policy, you are entitled to a free disclosure if you believe there may be fraudulent information on your credit report as a result of identity theft or other fraud, and so that is part of our phone script and part of our Internet scripting as well. So, I can't, you know, reply in particular. Obviously, we will be happy to follow up and—if, I mean, if it was our company, we would be happy to refund or whatever.

Mr. GREENWOOD. Is a credit bureau report easy for a layperson to read and understand? You heard Ms. Kane saying that sometimes there are abbreviations, there aren't necessarily numbers, toll-free numbers that can be gleaned from the report. Would I really know what to look for on my credit bureau report to determine whether I had been a victim of identity theft?

Mr. RYAN. I may be a bit biased, Mr. Chairman, because I have been in the business so long, but when I—we have done a lot of

work and testing of our consumer disclosure form. It is not the same credit report that would go to a bank, or you know, other financial institutions, so it is recast in English, and we do explain the different sections, so it is as clear as a very—typically long, 6, 7, 8 page, rather arcane listing of financial information, dates and dollar amounts can be, in my opinion.

Mr. GREENWOOD. Okay. Another one of the major problems we hear regarding victims of identity theft is that they usually did not discover the theft for a long time, in some cases, for over a year. The question is what type of fraud detection systems or services could the credit bureaus provide to try and identify the fraud before the victim even becomes aware of it?

Mr. RYAN. We are, as an ongoing matter of our business practice, we are looking at better ways to alert all of our constituents to possible fraud. We maintain, though, again, files on 220 million—all the credit active people in the United States, and so, I don't—we have not identified a way to proactively notify individual consumers. We certainly do—we are very available, you know, we are very open. And the new FACT Act, again, provides a free annual disclosure to everybody in the country, plus, as again, as I said, we have been open and available to providing free disclosures to consumers who even think there may be fraudulent information on their file. But—and that's the state-of-the-art pretty much today on this.

Mr. GREENWOOD. Are there provisions that you would have preferred to see get into the FACT Act that were not?

Mr. RYAN. I think that—no, the FACT Act is—it is a very comprehensive law. If, Mr. Chairman, you are asking if there are other issues pertaining to identity theft, that as a matter of public policy or legislation, were not addressed in the FACT Act, you—the committee has heard some of those earlier today. One is the issue of the robustness of our State identification, the driver's license system and ID cards and there is certainly legislation in Congress or it has been considered in Congress, aid to the states in making—providing for a more robust, perhaps biometric base identification system.

Mr. GREENWOOD. I think that is where we are headed. That has been what has been going through my mind this morning is that eventually, we are going to have to—as a technological response that we are going to have to go to a more sophisticated system, that uses some kind of biometrics in order to really protect our financial security. Is that where you think we are headed?

Mr. RYAN. That is where—that is at least one public policy issue that certainly is appropriate for Congress and perhaps this Committee to consider. Another issue that you heard mentioned earlier that I—we fully support are more resources for law enforcement for both data sharing, the FTC and the FBI, the Postal Inspector are all doing a lot, and as you also heard, the record is more uneven in the states. You know, some are doing more than others, but data sharing——

Mr. GREENWOOD. Do you think some states are doing too much? You know, there is an issue that I asked Representative O'Neill, which is how he felt about the Federal Government superseding the State laws, and I know California particularly felt that their

law was more stringent and they weren't happy about having it superseded by the Federal Law. Is that your experience?

Mr. RYAN. Well, I think the FACT Act got the preemptions on identity theft about right, Mr. Chairman. The preemptions were very narrow. They only—what got preempted by the FACT Act were the national standards for the security alerts, for example, or the national standards for the trade line blocking with a police report, and to us, it makes a lot of sense to have one national standard for how security alerts work.

And apart from the benefits to business, the benefit is to consumer empowerment, consumer education. So this way, what gets published in the FTC education program that they will—they are going to be working on in the next year or so, we will have a national standard, and one way security alerts and military active duty alerts operate one way. But in other areas, the preemptions were not there. The preemptions were narrow. I think they got it about right.

Mr. GREENWOOD. Let me—before I turn to Mr. Gerlach, let me just ask some questions of Ms. Lenahan. When you look at the 20 cases that you are investigating, could you give us a sense of—you mentioned one specific act where someone will come in to one of your branches with a stolen check, let us say, and write the check to himself for $500 and then deposit $50 and take $450. Are the crimes that you are investigating, do they tend to actually occur in your branches where people walk in and do that, or is it more the case that they are just figuring out how to drain someone's account from an ATM machine, for instance?

Ms. LENAHAN. I would say that it is probably about even. We have about—we have 12 locations in Bucks County only, and usually, what happens is if we happen to be unfortunate enough to get hit inside the branch, it is all within a day. And they go from location to location, and——

Mr. GREENWOOD. Have your video cameras or your security cameras ever assisted in the——

Ms. LENAHAN. Yes. Yes, they have.

Mr. GREENWOOD. That is interesting.

Ms. LENAHAN. We have an excellent system called AccuTrack, and it provides beautiful pictures.

Mr. GREENWOOD. So you can match, obviously, the transaction with the——

Ms. LENAHAN. Yes, we can.

Mr. GREENWOOD. [continuing] time of the transaction?

Ms. LENAHAN. Yes, we can.

Mr. GREENWOOD. To the place with the—that moment in your videotape and try to identify the person on there.

Ms. LENAHAN. Yes, we can.

Mr. GREENWOOD. When I go to an ATM machine and forget to say no, I don't want a receipt and a receipt comes out, and I crumple it up and stick it in that little slot that says trash. Do I have to worry about that receipt being used for fraudulently?

Ms. LENAHAN. No, you do not. It only lists the last four digits of the debit card number.

Mr. GREENWOOD. Which brings me to another point. One of the things I have learned in this investigation is that, of course, the

ideal is to have a truncated—in every transaction, to have a truncated credit card number, so you just have the last four numbers indicated and then lots of Xes, but not every vendor uses that, because it can be costly to have equipment that does that. And so, the perpetrator can make a purchase—well, it is—a purchase can be made in a—let us say, a smaller retail shop that doesn't truncate that information. That receipt can be picked up by a perpetrator, taken to a department store, and that number used there to perpetrate a crime on another retailer, and so the retailer who may have a truncated system is being victimized as a result of the fact that the smaller retailers don't.

Ms. LENAHAN. Right.

Mr. GREENWOOD. And that is a problem. And it is not easily solved, because it is tough—because of the cost of that equipment, it is tough to mandate that all retailers do that. It is tempting to do that, but it is expensive for the——

Ms. LENAHAN. You only need the credit card number. If that happened in a location, you wouldn't be able to take that piece of carbon number, or the number and go make a physical purchase.

Mr. GREENWOOD. Right. You don't need to.

Ms. LENAHAN. But——

Mr. GREENWOOD. You can go online and go to Macy's and——

Ms. LENAHAN. Online, telephone.

Mr. GREENWOOD. [continuing] buy stuff all day long.

Ms. LENAHAN. Right.

Mr. GREENWOOD. What types of security measures does your make take to ensure that your bank employees who have access to customers' personal information, are not abusing that information and potentially committing identity theft?

Ms. LENAHAN. Well, we are all bound to a code of ethics, and I don't think that there is anybody that is scrutinized more closely than our own employees. I am not going to say that is 100 percent foolproof, but in my experience, I have not had any experience in the last—since May 2002, of any negativity on an employee's end. Everything is security code and password sensitive. There is reports that we receive on a daily basis that are security department reviews, which includes employees' account activity. So it is watched.

Mr. GREENWOOD. Okay. Mr. Gerlach, questions?

Mr. GERLACH. A couple questions, thank you. Mr. Ryan, first, I am just looking at your testimony. On page 4, "The FACT Act also codifies what has been our industry's voluntary practice concerning the immediate blocking of information related to identity theft upon the consumer's providing us with an identity theft report—usually a police report. This practice is also known as 'tradeline blocking'". Can you describe that a little bit more fully for me, what "tradeline blocking" is, when a consumer says he or she is a victim of theft, perhaps gives you a police report? What do you do at that point?

Mr. RYAN. Yes. Yes, I can, Congressman. The process typically begins when we provide the consumer a free copy of their complete credit report, so they—so in other words, the first step is the prospective identity theft victim, or the victim contacts us. We give them a copy of the free report. They may or may not at that point

have a police report, but then at some point thereafter, or if they don't already have it, they get a police report, or a report by the U.S. Postal Service, or some other official document documenting the—make sure the fact of the identity theft. At that point, our consumer relations department, our Fraud Victim Assistance folks will receive from—the consumer tells us this, this, this and this item either trade—a trade line is a record of an account, so a Citibank, a record of the Citibank charge account or a Sears charge account.

Mr. GERLACH. Right.

Mr. RYAN. Or an inquiry could be associated—on the file could be associated with fraud. In other words, an—just the record of an inquiry by an institution that again, the consumer informs us is not a place they applied to, and therefore associated with a fraud. What happens in those cases of each element of information that is identified by the consumer, at that point gets suppressed from display. It gets blocked from display, so that it does not appear, can not appear on any future credit report, and we initiate a notice to the furnisher of each of those—the institution that furnished each of those elements of information, informing them that the data has been blocked from display, won't appear on future credit reports, has been associated to be connected with identity theft, and then they are—they have an opportunity, or an obligation, under the Fair Credit Reporting Act, to initiate their own investigation and take steps to not reintroduce it in subsequent reports to the credit reporting agency. Obviously, if they have—in their investigation, feel there is—that it was not identity theft, or it was some other kind of fraud going on there, there may be—they may come back to us, but the ordinary process stops there with our notice to them and their prevention of having it reintroduced.

Mr. GERLACH. Okay. So, at this point, the consumer can initiate that simply by having noticed this information on the report, and you take that individual's objection to that information on face value, and you block it.

Mr. RYAN. Once they have a police report. Yes, with a police report.

Mr. GERLACH. Okay. And the police report being simply an incident report that they have gone, made contact with the local police, explained the situation to the police, issues a report, not necessarily a finding of——

Mr. RYAN. No.

Mr. GERLACH. [continuing] criminality, or any of that sort, but that is—that paper is sufficient for you then to block that item for future use of that report by some other entity.

Mr. RYAN. Yes, Congressman.

Mr. GERLACH. Okay.

Mr. RYAN. And again, that has been our practice for several years, and that is now codified under the FACT Act.

Mr. GERLACH. Right. Okay. Real quick, Ms. Lenahan. We have heard information where the Mexican consulate could issue what is called a matricula consular card to those coming from Mexico and to have that card be the basis for coming into a bank and establishing an account and starting transactions through that account, but the individual that went into the consulate to say I am

so and so uses a birth certificate that may or may not be valid or genuine or authentic and nonetheless gets that consular card that is then used to open up accounts. Are you aware of any problems with that in your area? I know you are out of Newtown Square. Are you aware of any problems with banks and how they, if at all, try to further evaluate the proper identity of the person that tries to open up an account and start undertaking financial transactions on that basis of that card that was used initially?

Ms. LENAHAN. I am not familiar with that particular instance, but I would have to say that the Customer Identification Program would eliminate somebody being able to come in and just use that one card only. They would have to come up with several other forms of identification to conduct any type of business like that.

Mr. GERLACH. Okay. So the card itself is not a sufficient enough basis for opening an account. At least at your bank?

Ms. LENAHAN. Not at my bank.

Mr. GERLACH. Or are you aware of any other——

Ms. LENAHAN. I can't speak for the industry. American Bankers Association may be able to get back to you for the record.

Mr. GERLACH. Okay.

Ms. LENAHAN. In reference to the industry. But in my bank, they would need more than that.

Mr. GERLACH. Okay. Good. Thanks. Just a couple more questions. Do either of you, from your association or personal experience, use an estimate or see numbers that would estimate either how much it is costing the Nation as a whole a year from identity theft, or what theft comes down to as a household? Seen these numbers?

Mr. RYAN. The—I think, Mr. Chairman, the RTC will—the recent report had some number—figures there, but they don't stick—it is millions and millions, but——

Mr. GERLACH. Well, the numbers that I have seen——

Mr. RYAN. [continuing] I don't have that number in my head.

Mr. GERLACH. [continuing] are credit card theft, about $33 billion a year, and total identity theft numbers on an order of magnitude of $50 billion a year, and my math tells me that that is several hundred dollars a household, that every household in America is paying several hundred dollars more a year, which would be good about this time of year to have in your pocket instead of having to put out, but that is what we are paying to go shopping in the extra cost of goods that comes from this.

Just a couple more questions. Ms. Lenahan, what is the banking industry as a whole doing about this? Do you have a sense of that? Is this the kind of thing that financial institutions are either—do you talk to your other—your fellow bankers from Bucks County or national conventions, is this a big part of what participants might be engaged in in educating themselves about?

Ms. LENAHAN. It is all of the above. I just attended a large security conference in Texas, and it covered several things, including the biometrics that you were speaking of, which we see that as a future trend. Banks are continually researching new software that would be compatible with their own to combat these types of things and catch them before they accelerate. My bank does not offer a credit card, so we don't see what the rest of the industry is seeing

in reference to the credit card theft. However, we do offer the Visa check card, and that in itself, you know, we do have our fraud instances with those, but we are a little more fortunate than the bigger guys, because we don't offer the credit card, per se. But——

Mr. GERLACH. Well, somebody—suppose somebody does what is very easy now, every—most of us in this room probably, when you go home today, will find at least a couple of lovely offers of free credit cards that we don't even open any more and just throw in the trash, and they become pretty easy for somebody to pick up and fill out and send in and get a credit card. If somebody fills one of those out with my name on it and gets a credit card with my name in it and walks into your bank, and says I would like to put $1,000 on my Visa card, what does your bank do to make sure that that doesn't happen to me?

Ms. LENAHAN. If it is an outside credit card, we are relying on the credit card company to give us the appropriate authorization, because that is the only tool that we have. For our own card, we would have had to have identified them through the Customer Identification Program before we would even process their application, so——

Mr. GERLACH. If someone gets—suppose if someone gets an extra copy, it wouldn't be difficult for someone to report to—taking my place, that I—they lost a credit card, and ask for copies to be sent, or pick up my credit card when it comes in the—when it is renewed and it comes in the mailbox, to pick that up and then go into a bank and it—I would assume that the authorization would sail through.

Ms. LENAHAN. Well, any new cards that are coming through the mail have a sticker on it with an 800 number for activation that you can only use from your home telephone. So that is one feature that is in place to protect the consumer.

Mr. GERLACH. Okay, so that seems to work pretty well, then, I guess.

Ms. LENAHAN. Right. I think that the most difficulty right now with credit card mailing is the ready access checks, get 0 percent if you use these checks. If the consumer doesn't open the envelope, they are throwing away a checkbook, you know, which is very easy for somebody else to pick up and try and use.

Mr. GERLACH. That is an interesting point. Nowadays, I can tell—there are things I can do so that I don't get certain kinds of junk phone calls. Are there things that consumers can do if you don't want to get any more of these checks, for instance, because I get them all the time, and I try to remember to tear them up before I discard them, but I don't always open the envelopes, and I am not giving my address out at this hearing, but—can you—can a consumer avoid being sent those kinds of free checks?

Ms. LENAHAN. Well, the—they can contact their credit card company and just simply ask them to stop, and you don't usually receive those types of checks until you already have an account with that credit card company. It is after that that you start to get a lot of the mailing, use the checks, get this percentage rate. But there is——

Mr. GERLACH. I get checks from credit cards I haven't had in 10 years.

Ms. LENAHAN. Well, that is—they still have you—you didn't close the account.

Mr. GERLACH. Right.

Ms. LENAHAN. I would recommend closing an account for any card that you are not using. But the State has the Do Not Call list, which is supposed to include mailing as well, but I do not believe that that covers an existing account, an open account.

Mr. GERLACH. Mr. Ryan, did you have any comment on any of that?

Mr. RYAN. No, I think that is exactly my sense.

Mr. GERLACH. Okay. Well, that is it. Okay. Thank you both——

Ms. LENAHAN. Thank you.

Mr. GERLACH. [continuing] very much for your testimony. It has been very helpful.

Mr. GREENWOOD. We are going to take about a 5-minute break before we call our next panel.

[Brief recess]

Mr. GREENWOOD. Okay. The committee will come to order, and I see that our third panel has arrived, and they are Ms. Betsy Broder of the Federal Trade Commission. She is the Assistant Director of the Division of Planning and Information of the Bureau of Consumer Protection from Washington; Mr. Kevin Burke, who is the Deputy Chief Postal Inspector for Eastern Field Operations, here in the—he is a U.S. Postal Inspector here in Langhorne, Pennsylvania, welcome; Mr. John M. Abel is the Pennsylvania Attorney General—from the Pennsylvania Attorney General's Office, Senior Deputy Attorney General, Bureau of Consumer Protection, welcome, sir thank you for coming here from Philadelphia; and from the State Police, we have Lieutenant Colonel Ralph M. Periandi. Am I saying that right?

Mr. PERIANDI. Yes, sir.

Mr. GREENWOOD. Okay. He is a Deputy Commissioner of Operations from Harrisburg, and we thank you for coming. As you have heard me say to the other witnesses, we take testimony in this Subcommittee under oath, and I have to ask if any of you object to giving your testimony under oath. Okay. You are, also pursuant to the rules of the committee and the House of Representatives, entitled to be represented by counsel. Any of you wish to be represented by counsel? You all have good clear consciences. No need for that. Okay, in that case, if you would stand and raise your right hands, please.

[Witnesses sworn.]

Mr. GREENWOOD. Okay. You are all under oath, and we will begin with Ms. Broder. Welcome and thank you for your testimony. You want to take that microphone there, not that one. You want them both near. The stenographer needs the one on the little white triangle, but you need to speak clearly into that one.

Ms. BRODER. Thank you, and——

Mr. GREENWOOD. And it is—thank you.

TESTIMONY OF BETSY BRODER, ASSISTANT DIRECTOR, DIVISION OF PLANNING AND INFORMATION, BUREAU OF CONSUMER AFFAIRS, FEDERAL TRADE COMMISSION; KEVIN J. BURKE, DEPUTY CHIEF INSPECTOR FOR EASTERN FIELD OPERATIONS, U.S. POSTAL INSPECTOR; JOHN M. ABLE, PENNSYLVANIA ATTORNEY GENERAL; AND LT. COL. RALPH M. PERIANDI, DEPUTY COMMISSIONER, OPERATIONS, PENNSYLVANIA STATE POLICE

Ms. BRODER. Good morning, Mr. Chairman and Congressman Gerlach.

Identify theft has become a consumer protection issue of dramatic proportions. As has been earlier stated, the numbers are staggering. Within the space of 1 year, almost 10 million persons suffered some form of identity fraud, from the misuse of an existing account to the complete takeover of their identity by opening new accounts, obtaining government benefits, or even filing for bankruptcy.

In addition to the trauma to the victims, which cannot be underestimated, this crime costs our society over $53 billion in the space of 1 year, with an additional 300 million hours spent by victims trying to undo the damage. We appreciate the opportunity to describe today some of the initiatives the FTC has undertaken to respond to this growing problem.

The Federal Trade Commission has been playing a key role in addressing identity theft and the problem it spawns well before the enactment of the Identity Theft and Assumption Deterrence Act of 1998, but that Act directed us to take a more central role in working with victims, educating the public, coordinating with law enforcement, criminal law enforcement in particular, and working with the private sector.

For consumers, we offer victim assistance through our toll-free hotline at 877-IDTHEFT and our online complaint form and other resources at consumer.gov/idtheft. Through either of these portals, consumers provide us with information concerning the episode of identity theft, and our trained phone counselors guide them through the steps that they need to take to start repairing the damage done by the theft and reducing the risk of any additional harm. Online consumers can obtain the same information from the materials we have posted on our website. The ID Theft site also links to our identity theft affidavit, a uniformly accepted affidavit that victims can use to dispute fraudulently opened accounts. This takes the place of the cumbersome process which I think Ms. Kane referred to, of filling out separate and distinct forms for each of the fraudulently opened accounts. It makes the recovery that much easier, and a copy of the affidavit is contained in our identity theft book, When Bad Things Happen to Your Good Name. We have an additional identity theft piece, What's It All About, which is a practical guide for identity theft, a condensed version of our identity theft major publication, both of which are available in both English and Spanish.

We want consumers to be empowered to take the steps that they need to to safeguard their identity, to be mindful of how they make information about themselves available online and off, to take care in how they make their personally identifying information avail-

able, how they handle our trash to whether they put firewalls up and engage in commerce on the Internet carefully and with due regard for their identifying information.

I would just like to point out, Mr. Chairman, that you have made great use of our resources online by linking directly from your home site to our identity theft information, the booklets and the affidavit. This is exactly what we are trying to do, to leverage our resources, so that others make them available to audiences that we might not be able to reach. We appreciate very much all of your fine efforts in that regard.

The FTC's role also extends to supporting criminal law enforcement and prosecution of these crimes. The FTC is a civil agency. We do not have jurisdiction to enforce the identity theft law, but our colleagues, some of whom are represented at this table, do.

I mentioned that identity theft victims, when they contact us either by the phone or online, provide information about the incident of identity theft. That information we enter into our Identity Theft Data Clearinghouse, and we share it with law enforcement agencies around the country. Almost 800 individual agencies, representing thousands of investigators, can log on to this site through a secure Internet connection and get access to the more than 400,000 identity theft complaints that we have received and also that have been sent to us by the Social Security Administration Office of Inspector General.

So law enforcement agencies from the Bucks County and Montgomery County District Attorney's Office, to the U.S. Postal Inspection Service nationwide, to a cop in the Los Angeles Police Department can see the big picture. They are all logging on to the same data at the same time. This aggregated data takes the place of the individual complaints that may have come across their desks, so rather than just seeing that one complaint from the one person, they are able to add to that complaint by searching the data base, and seeing how pervasive the problem is, making ID theft more attractive for prosecution.

We have also teamed with the Inspection Service, the Secret Service and the U.S. Department of Justice to conduct training for law enforcement around the country. We have reached more than 1,000 of these first responders—with guidance on how to deal with identity theft victims, and how to build a case for prosecutors. So hopefully, what this means is that the story that we heard from Mrs. Kane about how the law enforcement would not listen to her, hopefully that tide is changing. They are looking at the individual as a victim of this crime, not simply the financial institutions that may have ultimately to carry the financial weight, but also, the person whose information has been misused are victims.

The International Association of Chiefs of Police have passed a resolution urging their members to take police reports in the jurisdiction where the victim resides. That is the one thing that remains constant. The thief may be operating in many jurisdictions, making it very hard for law enforcement to nail it down, but the victim always remains where she is, and so the police departments in the municipality of the victim are urged to issue police reports. That is of even greater importance now that we have the Police Re-

port Blocking Initiative. The police report is an essential piece of recovery for victims of identity theft.

One other point on law enforcement. We provide our data in the central data base that can be accessed by investigators one by one, but we also reach out with more specialized assistance. For example, the Identity Theft Task Force in Philadelphia requested, and we provided, a set of data from our data base that matched their jurisdictional range, so what we did was we took from our data base the complaints pertaining to that jurisdiction in the Philadelphia area, and I think there are other jurisdictions represented on that Task Force. They add to that some of their own data, so they have richer resources to drill further into this crime and build better cases. We work both in the collective and the individual groups on rooting out this pervasive crime.

And finally, the business community plays a key role in reducing the incidence of identity theft and working with victims. In addition to using and accepting the identity theft affidavit, the FTC has worked with companies who themselves have had their customers' or clients' data stolen, for example, the Red Cross. We provide direction to those companies on how to contact the persons whose information has fallen into the hands of criminals. The FTC staff also guides them to the appropriate law enforcement agency, and to work with the credit reporting agencies, so they can build together a mechanism to facilitate the recovery for the victims, and to provide them with the appropriate notice.

We also have drafted a standard letter for these companies to use in sending out to the people whose information has been compromised, so they get all of the appropriate contact information. They don't have to do their own homework or discover it for themselves. It also provides them with a link to our identity theft materials.

We know that these sorts of wholesale incidents of identity theft are becoming more commonplace, so rather than have our staff on the phone each and every time this happened, we have built an Identity Theft Response Kit that is posted on our home site that companies can go to to download the contact letter to see how to contact the credit reporting agencies and law enforcement as well, to make it easier for them to do their job.

Finally, the recent amendments to the FCRA, the FACT Act, including the codification of the fraud alert process with the credit reporting agencies, and the development of what are called red flag indicators of identity theft for financial institutions will certainly have an impact on this daunting crime. But clearly there is much that remains to be done, and the FTC will continue to make this a priority of its work.

We thank you very much for the opportunity to testify today.

[The prepared statement of Betsy Broder follows:]

PREPARED STATEMENT OF BETSY BRODER, ASSISTANT DIRECTOR, DIVISION OF PLANNING AND INFORMATION, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

I. INTRODUCTION

Mr. Chairman, and members of the Subcommittee, I am Betsy Broder, Assistant Director of the Division of Planning and Information, Bureau of Consumer Protec-

tion, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the impact of identity theft on consumers.

The Federal Trade Commission has a broad mandate to protect consumers, and controlling identity theft is an important issue of concern to all consumers. The FTC's role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").[2] The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints, to make available and to refer these complaints to law enforcement for their investigations, and to provide victim assistance and consumer education. Thus, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.[3] The Commission also works extensively with industry on ways to improve victim assistance, including providing direct advice and assistance in cases of security breaches involving sensitive information of customers or employees.

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

The Identity Theft Act strengthened the criminal laws governing identity theft[4] and focused on consumers as victims.[5] In so doing, Congress recognized that coordinated efforts are essential to best serve the needs of identity theft victims because these fraud victims often need assistance both from government agencies at the national and state or local level and from businesses. To fulfill the Act's mandate, the Commission implemented a program that focuses on three principal components: (1) collecting complaints and providing victim assistance through a telephone hotline and a dedicated website; (2) maintaining and promoting the Identity Theft Data Clearinghouse (the "Clearinghouse"), a centralized database of victim complaints that serves as an investigative tool for law enforcement; and (3) providing outreach and education to consumers, law enforcement, and private industry on prevention of identity theft.

A. Understanding Identity Theft

On November 1, 1999, the Commission began collecting complaints from consumers via a toll-free telephone number, 1-877-ID THEFT (438-4338) ("ID Theft hotline"). Every year since has seen an increase in complaints.[6] The Clearinghouse now contains over 400,000 identity theft complaints from victims across the country. By itself, though, this self-reported data does not allow the FTC to draw conclusions about the incidence of identity theft in the general population. Consequently, the FTC commissioned a survey to get a better picture of the incidence of identity theft

---

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

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

[3] Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by Section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. Corporate Marketing Solutions, Inc.,* CIV-02 1256 PHX RCB (D. Ariz. Feb. 3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards) and *FTC v. C.J.,* CIV-03 5275 GHK (RZx) (C.D. Cal. July 24, 2003) (final order) (defendant sent spam purporting to come from AOL and created an AOL look-alike website in order to obtain credit card numbers and other financial data from consumers which defendant used for unauthorized online purchases.). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. Press Release, Federal Trade Commission, *FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam* (Jan. 16, 2003), available at http://www.ftc.gov/opa/2003/01/idpfinal.htm.

[4] 18 U.S.C. § 1028(a)(7). The statute broadly defines "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code, and telecommunication identifying information.

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

[6] Charts that summarize data from the Clearinghouse can be found at http://www.consumer.gov/idtheft/stats.html and

and the impact of the crime on its victims.[7] The results are startling. Identity theft is more widespread and pernicious than previously realized. The data show that within the 12 months preceding the survey, 3.2 million people discovered that an identity thief opened new accounts in their name. An additional 6.6 million consumers learned of the misuse of an existing account. Overall, nearly 10 million people—or 4.6 percent of the adult population—discovered that they were victims of some form of identity theft. These numbers translate to nearly $48 billion in losses to businesses, nearly $5 billion in losses to victims, and almost 300 million hours spent by victims trying to resolve the problem. Moreover, according to the researchers, identity theft is a growing crime. The survey indicates a significant increase in the past 2-3 years—nearly a doubling from one year to the next, although the research shows that the rate of increase slowed during the past 1-2 years. It also is worth noting that most of the recent increase primarily involves the account takeover form of identity theft that tends to cause less economic injury to victims and is generally easier for them to identify and fix. Overall, the survey puts the problem of identity theft into sharper focus, and has spurred the FTC to even greater efforts to help victims and support law enforcement in its aggressive prosecution of identity thieves.

B. Assisting Identity Theft Victims

In addition to taking complaints from victims, the FTC provides advice on recovery from identity theft. Callers to the ID Theft hotline receive telephone counseling from specially trained personnel who provide general information about identity theft and help guide victims through the steps needed to resolve the problems resulting from the misuse of their identities.[8] Victims are advised to: (1) obtain copies of their credit reports from the three national consumer reporting agencies and have a fraud alert placed on their credit reports;[9] (2) contact each of the creditors or service providers where the identity thief has established or accessed an account, to request that the account be closed and to dispute any associated charges; and (3) report the identity theft to the police and get a police report, which is very helpful in demonstrating to would-be creditors and debt collectors that the consumers are genuine victims of identity theft.

Counselors also advise victims having particular problems about their rights under relevant consumer credit laws including the Fair Credit Reporting Act,[10] the Fair Credit Billing Act,[11] the Truth in Lending Act,[12] and the Fair Debt Collection Practices Act.[13] If the investigation and resolution of the identity theft falls under the jurisdiction of another regulatory agency that has a program in place to assist consumers, callers also are referred to those agencies.

The FTC's identity theft website, located at www.consumer.gov/idtheft, provides equivalent service for those who prefer the immediacy of an online interaction. The site contains a secure complaint form that allows victims to enter their identity theft information for input into the Clearinghouse. Victims also can read and download all of the resources necessary for reclaiming their credit record and good name. One resource in particular is the FTC's tremendously successful consumer education booklet, Identity Theft: When Bad Things Happen to Your Good Name. The 26-page booklet, now in its fourth edition, comprehensively covers a range of topics, including the first steps to take for victims, how to correct credit-related and other problems that may result from identity theft, tips for those having trouble getting a police report taken, and advice on ways to protect personal information. It also describes federal and state resources that are available to victims who may be having particular problems as a result of the identity theft. The FTC alone has distributed more than 1.2 million copies of the booklet since its release in February 2000, and recorded over 1.2 million visits to the web version.[14] Last year, the FTC

---

[7] The research took place during March and April 2003. It was conducted by Synovate, a private research firm, and involved a random sample telephone survey of over 4,000 U.S. adults. The full report of the survey can be found at http://www.consumer.gov/idtheft/stats.html.

[8] Spanish speaking counselors are available for callers who are not fluent in English.

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

[10] 15 U.S.C. § 1681 *et seq.*

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

[12] *Id.* § 1601 *et seq.*

[13] *Id.* § 1692 *et seq.*

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

released a Spanish language version of the Identity Theft booklet, *Robo de Identidad: Algo malo puede pasarle a su buen nombre.*

C. The Identity Theft Data Clearinghouse

Because one of the primary purposes of the Identity Theft Act was for criminal law enforcement agencies to use the database of victim complaints to support their investigations, the Commission took a number of steps to ensure that the database would meet the needs of law enforcement, before launching it. Initially, the FTC met with a host of law enforcement and regulatory agencies to obtain feedback on what the database should contain. Law enforcement access to the Clearinghouse via the FTC's secure website became available in July of 2000. To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaints from other sources. For example, in February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC with complaints from its fraud hotline, significantly enriching the FTC's database.

The Clearinghouse provides a picture of the nature, prevalence, and trends of the identity theft victims who submit complaints. FTC data analysts aggregate the data and develop them into charts and statistics.[15] For instance, the Commission publishes charts showing the prevalence of identity theft by states and by cities. Law enforcement and policy makers at all levels of government use these reports to better understand the challenges identity theft presents.

Since the inception of the Clearinghouse, more than 770 law enforcement agencies, from the federal to the local level, have signed up for access to the database. Individual investigators within those agencies have the ability to access the system from their desktop computers 24 hours a day, seven days a week. The Commission actively encourages even greater participation.

As previously stated, one of the goals of the Clearinghouse and the FTC's identity theft program is to support identity theft prosecutions nationwide.[16] Last year, in an effort to further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice, the United States Postal Inspection Service, and the United States Secret Service, initiated full-day identity theft training seminars for state and local law enforcement officers. To date, sessions have been held in Washington, D.C., Des Moines, Chicago, San Francisco, Las Vegas, Dallas, Phoenix, New York, Seattle, and San Antonio. The FTC also helped the Kansas and Missouri offices of the U.S. Attorney and State Attorney General conduct a training seminar in Kansas City. More than 1200 officers have attended these seminars, representing more than 300 different agencies. A session to be held in Orlando in January will commence next year's round of seminars.

The FTC staff also developed an identity theft case referral program.[17] The staff creates preliminary investigative reports by examining significant patterns of identity theft activity in the Clearinghouse and refining the data through the use of additional investigative resources. Then the staff refers the investigative reports to appropriate Financial Crimes Task Forces and other law enforcers located throughout the country for further investigation and potential prosecution. The FTC is aided in this work by its federal law enforcement partners including the United States Secret Service, the Federal Bureau of Investigation, and the United States Postal Inspection Service who provide staff and other resources.

D. Outreach and Education

The Identity Theft Act also directed the FTC to provide information to consumers about identity theft. Recognizing that law enforcement and private industry each play an important role in the ability of consumers both to minimize their risk and to recover from identity theft, the FTC expanded its outreach and education mission to include these sectors.

(1) *Consumers:* The FTC has taken the lead in coordinating with other government agencies and organizations in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive consumer and business edu-

---

[15] Charts that summarize data from the Clearinghouse can be found at http://www.consumer.gov/idtheft/stats.html and http://www.consumer.gov/sentinel/index.html.

[16] The Commission testified last year in support of S. 2541, the Identity Theft Penalty Enhancement Act of 2002, which would increase penalties and streamline proof requirements for prosecution of many of the most harmful forms of identity theft. *See* Testimony of Bureau Director J. Howard Beales, Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Government Information (July 11, 2002). S. 2541 has been reintroduced in the 108th Congress as S. 153.

[17] The referral program complements the regular use of the database by all law enforcers from their desktop computers.

cation campaign includes print materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, which includes the publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.

To increase identity theft awareness for the average consumer, the FTC recently developed a new primer on identity theft, *ID Theft: What's It All About?* This publication discusses the common methods of identity thieves, how consumers can best minimize their risk of being victimized, how to identify the signs of victimization, and the basic first steps for victims. Since its release in May 2003, the FTC has distributed almost 268,000 paper copies, and over 15,000 web versions. With the detailed victim recovery guide, *Identity Theft: When Bad Things Happen to Your Good Name,* the publication helps to fully educate consumers.

(2) *Law Enforcement:* Because law enforcement at the state and local level can provide significant practical assistance to victims, the FTC places a premium on outreach to such agencies. In addition to the training described previously (*see supra* Section II.C.), the FTC staff joined with North Carolina's Attorney General Roy Cooper to send letters to every other Attorney General letting him or her know about the FTC's identity theft program and how each Attorney General could use the resources of the program to better assist residents of his or her state. The letter encouraged each Attorney General to link to the consumer information and complaint form on the FTC's website and to let residents know about the hotline, stressed the importance of the Clearinghouse as a central database, and described all of the educational materials that each Attorney General can distribute to residents. North Carolina took the lead in availing itself of the Commission's resources in putting together for its resident victims a package of assistance that includes the ID Theft Affidavit (*see* Section II.D.(3)(b)), links to the FTC website and www.consumer.gov/idtheft. Through this initiative, the FTC hopes to make the most efficient use of federal resources by allowing states to take advantage of the work the FTC already has accomplished and at the same time continuing to expand the centralized database of victim complaints and increase its use by law enforcement nationwide. Other outreach initiatives include: (i) Participation in a "Roll Call" video produced by the Secret Service, which has been sent to thousands of law enforcement departments across the country to instruct officers on identity theft, investigative resources, and assisting victims and (ii) the redesign of the FTC's website to include a section for law enforcement with tips on how to help victims as well as resources for investigations.

(3) *Industry:* The private sector can help with the problem of identity theft in a number of ways. For instance, businesses can prevent identity theft by keeping their customers' or employees' sensitive information secure and out of the wrong hands. In addition, businesses can implement procedures to assist identity theft victims in the recovery process.

(a) *Information Security Breaches:* The FTC works with institutions that maintain personal information to identify ways to help keep that information safe from identity theft. Last year, the FTC invited representatives from financial institutions, credit issuers, universities, and retailers to an informal roundtable discussion of how to prevent unauthorized access to personal information in employee and customer records. The FTC will soon publish a self-assessment guide to make businesses and organizations of all sizes more aware of how they manage personal information and to aid them in assessing their security protocols.

As awareness of the FTC's role in identity theft has grown, businesses and organizations that have suffered compromises of personal information have begun to contact the FTC for assistance. For example, in the cases of TriWest[18] and Ford/Experian,[19] in which tens of thousands of consumers' files were compromised, the Commission gave advice on how to notify those individuals and how to protect the data in the future. To provide better assistance in these types of cases, the FTC developed a kit, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business,* that will be posted on the identity theft website in the coming weeks. The kit provides advice on which law enforcement agency to contact, business contact information for the three major credit reporting agencies, suggestions for establishing an internal communication protocol, information about contacting the FTC for assistance, and a detailed explanation of what information individuals need to know. The kit also includes a model letter for notifying individuals when their names and Social Security numbers have been taken. Organizations are encouraged

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

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

to print and include copies of *Identity Theft: When Bad Things Happen to Your Good Name* with the letter to individuals.

The FTC particularly stresses the importance of notifying individuals as soon as possible when information has been taken that may put them at risk for identity theft. They can then begin to take steps to limit the potential damage to themselves. For example, individuals whose Social Security numbers have been compromised, and who place a fraud alert promptly have a good chance of preventing, or at least reducing, the likelihood that the theft or release of this information will turn into actual misuse. Prompt notification also alerts these individuals to review their credit reports and to watch for the signs of identity theft. In the event that they should become victims, they can quickly take action to clear their records before any long-term damage is done. Besides providing *Information Compromise and the Risk of Identity Theft: Guidance for Your Business,* the FTC staff can provide individual assistance and advice, including review of consumer information materials for the organization and coordination of searches of the Clearinghouse for complaints with the law enforcement officer working the case.

(b) *Victim Assistance:* Identity theft victims spend significant time and effort restoring their good name and financial records. As a result, the FTC devotes significant resources to conducting outreach with the private sector on ways to improve victim assistance procedures. One such initiative arose from the burdensome requirement that victims complete a different fraud affidavit for each different creditor with whom the identity thief had opened an account.[20] To reduce that burden, the FTC worked with industry and consumer advocates to create a standard form for victims to use in resolving identity theft debts. From its release in August 2001 through October 2003, the FTC has distributed more than 293,000 print copies of the ID Theft Affidavit. There have also been nearly 479,000 hits to the web version. The affidavit is available in both English and Spanish.

Another initiative designed to assist victims is the "joint fraud alert" administered by the three major credit reporting agencies ("CRAs"). After receiving a request from an identity theft victim for the placement of a fraud alert on his or her consumer report and for a copy of that report, each CRA now shares that request with the other two CRAs, thereby eliminating the requirement that the victim contact each of the three major CRAs separately.

III. NEW PROTECTIONS FOR IDENTITY THEFT VICTIMS

On December 4, President Bush signed the Fair and Accurate Credit Transactions Act of 2003.[21] Many of the provisions amend the Fair Credit Reporting Act ("FCRA")[22] and provide new and important measures to prevent identity theft, enhance consumer ability to detect it when it does occur, and facilitate identity theft victims' recovery.[23]

A. Access to free consumer reports[24]

Previously, under the FCRA consumers were entitled to a free consumer report only under limited circumstances.[25] Now consumers have the right to request a free consumer report annually from nationwide CRAs. This benefit will enhance consumers' ability to discover and correct errors, thereby improving the accuracy of the system, and also can provide an early alert to identity theft victims about crimes committed in their names.

---

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

[21] Pub. L. No. 108-396 (2003) (codified at 15 U.S.C. § 1681 *et seq.*).

[22] 15 U.S.C. § 1681 *et seq.*

[23] The Commission testified on July 9 and 10, 2003 before the House Committee on Financial Services and the Senate Committee on Banking, Housing, and Urban Affairs respectively. The testimony can be found at http://www.ftc.gov/os/2003/07/fcratest.html and http:///www.ftc.gov/os/2003/07/fcrasenatettest.htm.

[24] Pub. L. No. 108-396, § 211 (2003).

[25] Previously, free reports were available only pursuant to the FCRA when the consumer suffered adverse action, believed that fraudulent information may be in his or her credit file, was unemployed, or was receiving welfare benefits. Absent one of these exceptions, consumers had to pay a statutory "reasonable charge" for a file disclosure; this fee is set each year by the Commission and is currently $9. *See* 15 U.S.C. § 1681j. In addition, a small number of states required the CRAs to provide free annual reports to consumers at their request.

B. National fraud alert system [26]

Under this provision, consumers who reasonably suspect they have been or may be victimized by identity theft, or who are military personnel on active duty away from home, can place an alert on their credit files. The alert will put potential creditors on notice that they must proceed with caution when granting credit in the consumer's name. The provision also codified and standardized the industry's "joint fraud alert" initiative (see Section II.D.(3)(b) *supra*).

C. Identity theft account blocking [27]

This provision requires CRAs immediately to cease reporting, or block, allegedly fraudulent account information on consumer reports when the consumer submits a police report or similar document, unless there is reason to believe the report is false. Blocking would mitigate the harm to consumers' credit records that can result from identity theft.

D. Truncation of credit and debit card receipts [28]

In many instances, identity theft results from thieves obtaining access to account numbers on credit card receipts. This source of fraud could be reduced by requiring merchants to truncate the full card number on the receipt. The use of truncation technology is becoming widespread, and some card issuers already require merchants to truncate. This law now requires truncation of credit and debit card numbers on electronic receipts, but creates a phase-in period to allow for the replacement of existing equipment.E. "Red flag" indicators of identity theft [29]

Under this provision, the banking regulators and the FTC will jointly develop guidelines for "red flag" indicators of identity theft. The goal of this provision is to give financial institutions and creditors up-to-date information on identity theft patterns and practices so that they can take appropriate action to prevent this crime.

IV. CONCLUSION

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

Mr. GREENWOOD. Thank you very much, Ms. Broder. Mr. Burke.

TESTIMONY OF KEVIN J. BURKE

Mr. BURKE. Good morning, Mr. Chairman and Congressman Gerlach. On behalf of the United States Postal Inspection Service, thank you for holding this hearing and giving me the opportunity to discuss the subject of identity crimes and the significant role postal inspectors play in combating it.

I am Kevin Burke, Deputy Chief Inspector for Eastern Field Operations for the Postal Inspection Service. The responsibility of safeguarding 200 billion pieces of mail and ensuring America's trust in the postal system falls squarely on the shoulders of the United States Postal Inspectors. As Federal law enforcement officers, we enforce over 200 Federal statutes. Primary among those are the theft or possession of stolen mail statute and the oldest, and still the most effective consumer protection law, the mail fraud statute.

Mr. GREENWOOD. I am sorry, we are going to need you to pull that microphone up.

---

[26] Pub. L. No. 108-396, § 112 (2003).
[27] *Id.* § 152.
[28] *Id.* § 113.
[29] *Id.* § 114.

Mr. BURKE. Last year, Postal Inspectors made over 11,000 arrests. 3,000 of those arrests were made for identity theft. Identity theft arrests have increased in each of the past 3 years.

I am sure all of you have received pre-approved credit applications in the mail. In the past, those mailings were prime targets for an identity thief, because they simply required the thief to sign the application and return it to the company. But times have changed, due to our efforts in raising awareness of the problem. For example, credit card companies have adopted recommendations we have made and have begun automatically discarding suspicious looking applications for credit, especially when there are differences between where the consumer claims they reside and what address their customer file indicates. In addition, credit card companies have changed another of their practices. Credit offers sent through the mail now contain much less information.

Another favorite vehicle for thieves used to be the fraudulent change of address scheme, directing the Post Office to forward a victim's mail to an address the thief controlled. Not any more. A proactive effort by the Postal Service to prevent a false change of address is the Move Validation Letter. Now, whenever a change of address is filed, the Postal Service sends a letter to both the new and old addresses. The letter instructs the recipient to call an 800 number if they have not recently requested a change. This simple measure has virtually eliminated the placing of false change of address with the Postal Service as an avenue for committing identity theft.

According to a report released by the FTC this past September, mail theft as a source of identity theft happened in only 4 percent of the cases surveyed. As we have made it more difficult for mail theft to be a component of identity theft, criminals have turned to other means, oftentimes recruiting the assistance of insiders, employees who have access to personal information of clients or other employees. Personal information contained in corporate and government records and computer data bases is a fertile area for dishonest employees working in conjunction with identity thieves.

Three years ago, a Philadelphia resident reported to police that after her father's death, she continued receiving credit card bills showing changes made in her father's name. The statements even reflected a request for a new account. U.S. Postal Inspectors and detectives from the Philadelphia Police Department determined that her father's identity had been stolen when his body was processed through the Medical Examiner's Office. 16 suspects were ultimately identified, 10 of them employees working within the Medical Examiner's Office. The employees used the credit cards to make purchases for themselves or passed the credit cards on and other personal information they found to outsiders. The scheme went on for 3 years before they got caught. All 16 defendants were caught and convicted. Postal Inspectors were called in to participate in the investigation as bills for illegally purchased items were sent through the mail, as was financial information for newly and fraudulently opened accounts.

Just last month, in a separate investigation, Postal Inspectors in Philadelphia and other task force member arrested the ringleader of an identity theft gang. A search of his Chester residence found

a commercial grade credit card embossing machine that the suspect had purchased over the Internet. The suspect used a fictitious name and had his purchase delivered by private courier to an abandoned Philadelphia area address, all without arousing suspicion. When searching his house, we also recovered 2,500 blank credit cards, numerous counterfeited credit cards, valid credit cards that had been stolen from the mail and counterfeit Pennsylvania, Virginia, Florida and District of Columbia drivers' licenses.

Postal Inspectors together with the FBI are also investigating the identity theft of about 30 Montgomery and Delaware County residents who donated blood to the American Red Cross in November or December of last year. Donors are required to supply their names, as was previously mentioned, Social Security number and other identifying information before giving blood. As was previously mentioned, this is a still active investigation, and I am not at liberty to discuss any details. However, I would like to commend the American Red Cross for their efforts in proactively—and assisting in this investigation.

In 2002, Patrick J. Meehan, U.S. Attorney for the Eastern District of Pennsylvania, formed a regional working group to facilitate the sharing of intelligence and investigative resources in combating identity theft in and around the Philadelphia area. As a member of the Group, the Postal Inspection Service has taken the lead in developing a web-based data base that tracks customer and financial industry reports of mail theft and identity theft. The data base allows all Group members to track loss information and perform advanced searches on victims' names. The data base also performs what is known as "link analysis," by automatically matching common addresses used by thieves.

One of the most insidious aspects of identity theft is the length of time the scheme can be carried out before it is even detected. It may be months before a victim realizes they have been targeted. It is not until a consumer gets turned down for credit, a car loan, or a mortgage on that dream house because of bad credit ratings that they realize what has taken place. Damaged credit ratings may take years to restore. Victims run the gamut of society. They are wealthy, they are poor, they are old and they are young. No one is immune. Anyone is a potential victim.

Aggressive law enforcement efforts are a key component of our mission. But arrests are not the only solution. We have found that creating awareness and prevention programs for consumers can go a long way to lessen the impact of this crime on the public.

Over the past 10 years, the Inspection Service has published and distributed a series of brochures and posters and newsletters to enhance and raise public awareness. Our publication Identity Theft—Safeguard Your Personal Information has been distributed to over 2 million consumers and businesses. Detecting and Preventing Account Takeover Fraud, another of our publications, advises credit card companies on steps they can take to detect and prevent takeover schemes.

Our most recent document is not going to be published, because it is an ever-changing, evolving document. It is called Fighting Identity Theft, and will be provided as a best practices to the finan-

cial industry, to law enforcement agencies and consumer groups and prosecutors throughout the United States.

Just this past September, the Postal Inspection Service, along with our partners in the FTC and the Postal Service, launched a nationwide awareness campaign on identity theft. We used a two-pronged approach, providing prevention and awareness information to consumers and informing businesses on the need to safeguard their files and data bases containing customer information. Actor Jerry Orbach, or television's Law and Order fame, who himself was a victim of identity theft, was the campaign's spokesman.

The Mullen agency of Pittsburgh provided support for this year's campaign on a pro bono basis. But what really makes this campaign unique is the funding source. We have all the saying "crime doesn't pay." In the case of this awareness campaign, it does pay. The campaign was funded with a unique application of fines and forfeitures paid by criminals in past fraud cased.

Sometimes, the most effective vehicle in getting out the message is when the message comes directly from an authoritative source, the criminals themselves. Last year, Postal Inspectors in Pittsburgh caught a man who stole the identities of several celebrities, including the actor Will Smith. The thief, Carlos Lomax, was prosecuted by the U.S. Attorney's Office in the Western District of Pennsylvania and convicted. Lomax agreed to let us tape an interview of him describing what he did and how he did it.

Educating the public and working to reduce opportunities where the Postal Service and the mail can be used for illegal purposes are crucial elements in our fight against identity crimes. As always, we will do our part to remove criminals from society. We appreciate the subcommittee's recognition of this important issue, and with your permission, sir, we would like to play a brief portion of that tape.

[The prepared statement of Kevin J. Burke follows:]

PREPARED STATEMENT OF KEVIN J. BURKE, DEPUTY CHIEF INSPECTOR, EASTERN FIELD OPERATIONS, UNITED STATES POSTAL INSPECTION SERVICE

Good morning, Mr. Chairman, members of the subcommittee. On behalf of the United States Postal Inspection Service, thank you for holding this hearing and giving me the opportunity to discuss the subject of identity crimes and the significant role Postal Inspectors play in combating it.

I'm Kevin Burke, Deputy Chief Inspector, Eastern Field Operations, for the Postal Inspection Service.

The responsibility for safeguarding 200 billion pieces of mail a year and ensuring America's trust in the postal system falls on the shoulders of U. S. Postal Inspectors.

As federal law enforcement officers, we enforce over 200 federal statutes; primary among those are the theft or possession of stolen mail statute and the oldest, and still the most effective consumer protection law, the mail fraud statute. Last year, Postal Inspectors made over 11,000 arrests. Three thousand of those arrests were for identity theft. Identity theft arrests have increased each year for the past three years.

I'm sure all of you have received pre-approved credit applications in the mail. In the past, those mailings were prime targets for an identity thief because they simply required the thief to sign the application and return it to the company. But times have changed, due to our efforts in raising awareness of the problem. For example, credit card companies have adopted recommendations we've made and have begun automatically discarding suspicious-looking applications for credit, especially when there are differences between where the "customer" claims they reside and what address their customer file indicates. In addition, credit card companies have changed

another of their practices—credit offers sent through the mail now contain much less information.

Another favorite vehicle for thieves used to be the fraudulent change-of-address scheme, directing the Post Office to forward a victim's mail to an address the thief controlled. Not any more. A proactive effort by the Postal Service to prevent a false change-of-address is the Move Validation Letter. Now, whenever a change-of-address is filed, the Postal Service sends a letter to both the old and new addresses. The letter instructs the recipient to call an "800" number if they had not recently requested a change. This simple measure has virtually eliminated the placing of a false change of address with the Postal Service as an avenue for committing identity theft.

According to a report released by the FTC this past September, mail theft as a source for identity theft happened in only 4% of the cases surveyed. As we have made it more difficult for mail theft to be a component of identity theft, criminals have turned to other means, oftentimes recruiting the assistance of insiders, employees who have access to the personal information of clients or other employees.

Personal information contained in corporate and government records and computer databases is a fertile area for dishonest employees working in conjunction with identity thieves.

Three years ago, a Philadelphia resident reported to police that, after her father's death, she continued receiving credit card bills showing charges made in her father's name. The statements even reflected a request for a new account. US Postal Inspectors and detectives from the Philadelphia Police Department determined that her father's identity had been stolen when his body was processed through the Medical Examiner's Office. Sixteen suspects were ultimately identified, ten of them employees working within the Medical Examiner's Office. The employees used the credit cards to make purchases for themselves or passed the credit cards and other personal information they found to outsiders. The scheme went on for three years before they got caught. All sixteen defendants were caught and convicted. Postal Inspectors were called in to participate in the investigation as bills for illegally purchased items were sent through the mail as was financial information for newly—and fraudulently—opened accounts.

Just last month, in a separate investigation, Postal Inspectors in Philadelphia and other task force members arrested the ringleader of an identity theft gang. A search of his Chester residence found a commercial-grade credit card embossing machine that the suspect had purchased over the Internet. The suspect used a fictitious name and had his purchase delivered by private carrier to an abandoned Philadelphia area address, all without arousing suspicion. When searching his house, we also recovered over 2,500 blank credit cards, numerous counterfeited credit cards, valid credit cards that had been stolen from the mail, and counterfeit PA, VA, FL and DC drivers' licenses.

Postal Inspectors together with the FBI are also investigating the identity theft of about 30 Montgomery and Delaware County residents who donated blood to the American Red Cross in November or December of last year. Donors are required to supply their names, social security numbers and other identifying information before giving blood. As this is still an active investigation, I am not at liberty to offer any details other than the Red Cross has been very forthcoming in cooperating with authorities and the case is ongoing.

In addition to modifying industry practices and making financial mailings less attractive to a thief, our partnerships with regulatory, financial industry and other law enforcement groups have resulted in a number of initiatives.

In 2002, Patrick J. Meehan, U.S. Attorney for the Eastern District of PA, formed a regional working group to facilitate the sharing of intelligence and investigative resources in combating identity theft in and around the Philadelphia area. As a member of the Group, the Postal Inspection Service has taken the lead in developing a web-based database that tracks customer and financial industry reports of mail theft and identity theft. The database allows all Group members to track loss information and perform advanced searches on victims' names. The database also performs what is known as "link analysis," by automatically matching common addresses used by thieves.

One of the most insidious aspects of identity theft is the length of time the scheme can be carried out before it is even detected. It may be months before a victim realizes they've been targeted. It's not until a consumer gets turned down for credit, a car loan or a mortgage on a dream house because of a bad credit rating do they realize what has taken place. Damaged credit ratings may take years to restore. Victims run the gamut of society—they're wealthy, they're poor; they're old, they're young. No one is immune. Anyone is a potential victim.

Aggressive law enforcement efforts are a key component of our mission. But arrests are not the only solution. We have found that creating awareness and prevention programs for consumers can go a long way to lessen the impact of this crime on the public.

Over the past 10 years, the Postal Inspection Service has published and distributed a series of brochures, posters and newsletters to raise public awareness. Our publication *"Identity Theft—Safeguard Your Personal Information,"* has been distributed to over two million consumers and businesses. *"Detecting and Preventing Account Takeover Fraud,"* another of our publications, advises credit card companies on steps they can take to detect and prevent takeover schemes.

Just this past September, the Postal Inspection Service, along with our partners the FTC and the Postal Service launched a nationwide awareness campaign on identity theft. We used a two-pronged approach: providing prevention and awareness information to consumers, and informing businesses on the need to safeguard their files and databases containing customers' information. Actor Jerry Orbach, of television's Law and Order fame, who himself was a victim of identity theft, was the campaign's spokesman.

The Mullen agency of Pittsburgh provided support for this year's campaign on a pro bono basis. But what really makes this campaign unique is the funding source. We've all heard the saying, "crime doesn't pay." In the case of this awareness campaign, it does pay. This campaign was funded through a unique application of fines and forfeitures paid by criminals in a past fraud case.

Sometimes the most effective vehicle for "getting out the message" is when the message comes directly from an authoritative source, the criminals themselves. Last year, Postal Inspectors in Pittsburgh caught a man who stole the identities of several celebrities, including the actor Will Smith. The thief, Carlos Lomax, was prosecuted by the U.S. Attorney's Office in the Western District of Pennsylvania and convicted. Lomax agreed to let us tape an interview of him describing what he did and how he did it. I would like to play a portion of that tape for you now.

Educating the public and working to reduce opportunities where the Postal Service and the mail can be used for illegal purposes are crucial elements in our fight against identity crimes. As always, we will do our part to remove criminals from society. We appreciate the subcommittee's recognition of the importance of this issue.

Mr. GREENWOOD. Please do.

[Video shown.]

Mr. GREENWOOD. Thank you. Mr. Abel, you are recognized for your statement.

TESTIMONY OF JOHN M. ABEL

Mr. ABEL. Good afternoon, Chairman Greenwood and Congressman Gerlach. On behalf of the Pennsylvania Attorney General, Mike Fisher, I am honored to be here this afternoon to testify on this important topic. My name is John Abel, and I am a Senior Deputy Attorney General in the Philadelphia Regional Office of General Fisher's Bureau of Consumer Protection.

Identity theft, as we heard, is a serious crime, and growing problem across the country with Pennsylvania's experience being no exception. Victim of this crime face devastating economic repercussions, and oftentimes spend countless hours undoing the harm in order to get their finances back in order. This can be a very stressful experience for the ordinary consumer, who in many instances does not realize until much later that their identity has been hijacked by an unknown perpetrator. By this time, hundreds if not thousands of dollars in unauthorized charges have been made in their name from any number of sources.

I am here today to speak on behalf of the Bureau of Consumer Protection that is housed within the Public Protection Division. By way of background, the Bureau has several regional offices which handle more than 40,000 written complaints annually from con-

sumers throughout the state. Nearly each of these consumer complaints is assigned to an individual agent, and in most instances, the agent will seek to mediate the case with the business, with the hopes of achieving a satisfactory resolution.

Should the Bureau detect a pattern or practice of consumer fraud, based on the complaint history or from any other source, the Bureau may then commence a formal investigation and take legal action if necessary. With regard to the issue of identity theft, I will focus, for my few moments, on the efforts of the Bureau in educating consumers to avoid these thieves, and assisting consumers with restoring their credit.

Although our office is vested with criminal authority to pursue perpetrators of identity theft, as a civil law litigator, I will not be able to speak specifically to the details of any criminal investigations or prosecutions. However, I would be happy to provide, later, any further information the subcommittee might desire.

As for the scope of the problem, according to the Social Security Administration, more than 750,000 incidents of identity theft occurred nationwide last year. One study found that on the average, it takes victims 175 hours and over $800 in out of pocket costs to clear their name.

Allow me to share with the committee some recent numbers which pertain specifically to Pennsylvanians. Statistics on identity theft are maintained by the Federal Trade Commission, which established an Identity Theft Hotline and Data Clearinghouse back in 1999. These records show that in 2002, Pennsylvania had reports of victims in 5,080 cases. The overwhelming majority, 46 percent, specifically experienced credit card fraud. Next, the most common instance involved unauthorized use of phone or utility services. Almost 1 in 4 of these crimes occurred in Philadelphia. However, every region of the State has experienced this brand of crime.

Data shows the typical victim of identity theft is between 30 and 40 years of age and does not notice the crime until roughly a year after they have become a victim. Particularly disturbing is the victimization of our seniors, who with their good credit, retirement nest eggs and trusting nature are often targeted by scam artists. Only the State of Florida has a higher percentage of citizens over the age of 65 than Pennsylvania, and Attorney General Fisher's efforts to protect the Commonwealth's citizens include a special commitment to the protection of our seniors.

As for efforts to combat the problem, the old saying that an ounce of prevention is worth a pound of cure is particularly true in this case. Attorney General Fisher has taken action to educate Pennsylvanians on how to avoid these tactics. Through various forms of outreach and public speaking, representatives from the Bureau help to spread the word on the rather simple and easy steps that consumers can take to avoid becoming a victim. We appear before religious and other community organizations, senior groups, numerous civic associations. We staff information booths at shopping malls and county fairs all throughout the state.

Just this last year, the Bureau joined the National Consumer Protection Week by participating in education fairs and activities throughout the state. The theme was "Consumer Confidential: The Privacy Story."

Consistent with what I had said about the seriousness of these crimes against seniors, the Attorney General's Office has also launched a program known as the Senior Crime Prevention University to educate older Pennsylvanians and their families on crime prevention. This program is presented in conjunction with other law enforcement agencies, who provide training to help stop the multitude of crimes, including identity theft against the senior citizens of Pennsylvania.

The Bureau has specially published a brochure with particular tips on how to protect one's personal identification information. For example, minimize identification information in cards you carry. Don't carry your Social Security card with you. Purchase a shredder. We have seen identity thieves that commonly sift through garbage seeking discarded mail. Be mindful of billing cycles. If it seems like one of your bills didn't arrive, follow up with the business. Don't give out personal information over the phone, through the mail, or over the Internet, unless you have initiated the contact or know with whom you are dealing. And last, order a copy of your credit report at least on an annual basis.

If, despite taking these precautions, a person's information does end up in the wrong hands, our Office then recommends taking the following steps immediately. Call the fraud departments of the credit bureaus and request that a fraud alert be put on your file. You should also ask for a copy of your credit report and then follow up with those bureaus by asking that they remove any fraudulent or incorrect information. Contact banks, credit card companies and all other creditors who issued credit in your name and/or permitted access to your existing account and close all affected accounts. Finally, then contact your local police department and file a criminal report on the incident.

As I mentioned before, each consumer complaint that the Bureau receives is assigned to an individual agent. In the case of identity theft, this agent is available to direct the consumer to the appropriate agencies. Additionally, these agents are available to work with and provide information to other parties in an effort to address some of the problems created by this theft.

The Bureau has also taken action within the context of legal actions to protect consumer privacy and avoid identity theft. For instance, when an online retailer of children's education materials announced that it was going to cease operations and sell off its assets, Pennsylvania, along with a majority of other states, filed an Objection in the Bankruptcy Court to prevent that company from selling its customer list. Ultimately, through the efforts of Pennsylvania, the FTC and 42 other states, this company agreed to destroy the customer list.

In another, more recent case, the Bureau took action against Bucks County based national seller of computers, and made certain that the settlement there prohibited the sale or disclosure of other consumer information.

Once again, thank you for the opportunity to comment today on the Bureau of Consumer Protection's efforts to assist consumers in preventing the growing problem of identity theft, and we want to commend Congress for its recent enactment of the Fair and Accu-

rate Credit Transactions Act, which should further assist consumers in combating this problem.

For instance, one of the two provisions that quickly come to mind is the one providing for a free annual credit report that will allow consumers to do this annual checkup that we talked—that we heard about this morning that is so important.

Another provision is the one that speaks to the truncation of credit card and debit card account information. These and the other provisions should assist in combating this problem.

I will be happy to take any questions.

[The prepared statement of John M. Abel follows:]

PREPARED STATEMENT OF JOHN M. ABEL, SENIOR DEPUTY ATTORNEY GENERAL, PENNSYLVANIA OFFICE OF ATTORNEY GENERAL, BUREAU OF CONSUMER PROTECTION

I. INTRODUCTION

Good morning Chairman Greenwood and distinguished members of the House Subcommittee on Oversight and Investigations. On behalf of the Pennsylvania Attorney General Mike Fisher, I am honored to be here this morning to testify on the important topic of identity theft. My name is John Abel and I am a Senior Deputy Attorney General in the Philadelphia Regional Office of General Fisher's Bureau of Consumer Protection.

Identity theft is a serious crime and growing problem across the country with Pennsylvania's experience being no exception. Victims of this crime face devastating economic repercussions and oftentimes spend countless hours undoing the harm in order to get their finances back in order. This can be a very stressful experience for the ordinary consumer who in many instances does not realize until much later that their identity has been hijacked by an unknown perpetrator. By this time, hundreds, if not thousands, of dollars in unauthorized charges have been made in their name from any number of sources.

I am here today to speak on behalf of the Bureau of Consumer Protection of the Attorney General's Office that is housed within the Public Protection Division. Along with the Bureau of Consumer Protection, a number of other offices are located within Public Protection including the Health Care Section, AntiTrust Section, Charitable Trusts and Organization Section and the Civil Rights Enforcement Section.

II. BACKGROUND

Before I begin to talk about this problem, let me start by giving you a brief background of the Bureau of Consumer Protection. By law, the Attorney General's Bureau of Consumer Protection is authorized to perform the following duties:

- Investigate commercial and trade practices in the distribution, financing and furnishing of goods and services for the use of consumers;
- Conduct studies, investigations and research into matters affecting consumer interests and make such information available to the public;
- Advise the Pennsylvania Legislature on matters affecting consumer interests, including the development of policies and the proposal of programs to protect consumers;
- Investigate fraud and deception in the sale, servicing and furnishing of goods and products, and strive to eliminate such illegal actions;
- Promote consumer education and publicize matters relating to consumer fraud, deception and misrepresentation.

The Bureau of Consumer Protection has seven regional offices which handle more than 40,000 written complaints annually from consumers throughout the Commonwealth. Over the past couple of years, the number of complaints has risen dramatically by more than 30 percent. This increase is due to a number of factors, one of which includes a growing wave of bankruptcies of a number of large retail establishments. Each of these consumer complaints is assigned to an individual agent and in most instances, that agent will seek to mediate the case with the business with hopes of achieving a satisfactory resolution. Should the Bureau detect a patten or practice of consumer fraud, based on complaint history or other sources, the Bureau may then commence a formal investigation.

Under the law, the Bureau is authorized to file a formal legal action where it has reason to believe that a business has engaged in such a pattern of illegal practices and it is in the public interest to do so. On average, the Bureau files 150 actions

per year. Legal actions take the form of a lawsuit filed in the Commonwealth Court or local Court of Common Pleas. These actions also include a settlement agreement permitted by law which is known as an Assurance of Voluntary Compliance. Through these actions, the Bureau can seek injunctive relief, such as prohibiting a company from doing business in the Commonwealth, as well as consumer restitution. The Bureau is authorized to seek a penalty of $1,000 per violation and $3,000 per violation where the consumer is of age 60 or older.

With regard to the issues of identity theft, I will focus on the efforts of the Bureau of Consumer Protection in educating consumers to avoid these thieves and in assisting consumers with restoring their credit. Although our Office is vested with criminal authority to pursue perpetrators of identity theft, as a civil law litigator with the office, I will not be able to speak specifically to the details of any criminal investigations or prosecutions. However, I would be happy to provide later any further information that the subcommittee might desire.

III. SCOPE OF PROBLEM

According to the Social Security Administration, more than 750,000 incidents of identity theft occurred nationwide last year. One study found that on the average, it takes victims 175 hours and over $800 in outofpocket to clear their name. The Federal Trade Commission reports that in 2002 they received 161,819 identity theft complaints. This national figure is almost double that which was reported in 2001, when the FTC tracked 86,198 complaints of identity theft. We have every reason to believe that the trend is increasing this year.

Allow me to share with the Committee some recent numbers which pertain specifically to Pennsylvanians. Statistics on identity theft are maintained by the Federal Trade Commission which established an Identify Theft Hotline and Data Clearinghouse in 1999. These records show that in 2002, Pennsylvania had reports of victims in 5,080 cases. The overwhelming majority, 46 percent, specifically experienced credit card fraud. Next to credit card fraud, the most common instance involved unauthorized use of phone or utility services. Almost 1 in 4 of these crimes occurred in Philadelphia. However, every region in the Commonwealth has experienced this brand of crime.

With statistics such as these, which have been steadily increasing, identity theft is a problem that certainly warrants the continued attention of the Subcommittee.

Data shows that the typical victim of identity theft is between 30 and 40 years old and does not notice the crime until roughly a year after they have become a victim. At this age, people generally have an established credit history and a steady income. Similarly, with children, work, and other commitments, there are a lot of priorities and responsibilities to tackle. It is often easy to take your financial privacy and security for granted. Particularly disturbing is the increasing victimization of our seniors who, with their good credit, retirement nest eggs and trusting nature, are often targeted by scam artists. Only the state of Florida has a higher percentage of citizens over the age of 65 than Pennsylvania, and Attorney General Fisher's efforts to protect the Commonwealth's citizens includes a special commitment to protection of our seniors.

These criminals use a variety of methods to access your information. They steal purses and wallets for personal information; they complete changeofaddress cards to have personal information forwarded out of the victim's hands. Other practices include "dumpster diving," where criminals steal discarded statements and preapproved credit offers from the victim's trash. "Shoulder surfing" refers to the practice of stealing PIN numbers and account numbers over the person's shoulder while they are using an ATM. Of course, the Internet is fertile ground for these thieves. A fraudulent email can be sent promising some benefit in exchange for personal information. A surprising number of people quickly sent out the information without taking any steps to determine the validity of the offer.

IV. EFFORTS TO COMBAT PROBLEM

The old saying that "an ounce of prevention is worth a pound of cure" is particularly true in the case of identity theft. Attorney General Fisher has taken action to educate Pennsylvanians on how to avoid these tactics. Through various forms of outreach and public speaking, representatives from the Bureau of Consumer Protection help to spread the word on the rather simple and easy steps that consumers can take to avoid becoming a victim. We appear before church and other community organizations, senior groups, as well as numerous civic associations. We staff information booths at shopping malls and county fairs throughout the state.

Just this last year, the Bureau joined in National Consumer Protection Week by participating in consumer education fairs and activities throughout the Common-

wealth. The theme was "Consumer Confidential: The Privacy Story." As part of this event, the Bureau rolled out a new brochure titled "Consumer Privacy: Protecting Your Personal Information."

Consistent with what I had mentioned about the seriousness of these crimes against seniors, the Attorney General's Office has also launched a program known as the Senior Crime Prevention University to educate older Pennsylvanians and their families on crime prevention. The Senior Crime Prevention University is presented in conjunction with other law enforcement agencies who provide training to help stop the multitude of crimes, including identity theft, against the senior citizens of Pennsylvania.

The Bureau has also specially published a brochure which offers specific tips to protect personal identifying information. For instance:

- Minimize the identification information and cards you carry. Don't carry your social security card with you and carry other cards that list your social security number (such as prescription cards or insurance cards) only when necessary.
- Purchase a shredder. As I said earlier, identity thieves commonly sift through garbage seeking discarded mail such as preapproved credit card offerings and bank statements.
- Be mindful of billing cycles if it seems like one of your bills didn't arrive, follow up with the business. Remember, that in addition to containing your name, address and other information, monthly statements also contain account numbers.
- Don't give out personal information over the phone, through the mail, or over the Internet unless you have initiated the contact, or know with whom you are dealing. To get your information, identity thieves may pose as representatives of banks, Internet services providers, even government agencies.
- Order a copy of your credit report.

If, despite taking these precautions, a person's information does end up in the wrong hands, our Office recommends taking the fallowing steps immediately:

- Call the fraud departments of the credit bureaus and request that a "fraud alert" be put on your file. This lets creditors know to call you before they open any new accounts in your name. You should also ask for a copy of your credit report and follow up with these credit bureaus by asking that they remove any fraudulent or incorrect information.
- Contact banks, credit card companies and all other creditors who issued credit in your name and/or permitted access to your existing account and close all affected accounts.
- Finally, contact your local police department and file a criminal report on the incident. Such a report can help in clearing up your credit records and, or course, may lead to the arrest of the thief.

As I mentioned before, each consumer complaint that the Bureau receives is assigned to an individual agent. In cases of identity theft, this agent is available to direct the consumer to the appropriate agencies. Additionally, the agents are available to work with, and provide information to, other parties in an effort to address some of the problems created by the theft.

The Bureau has also taken action within the context of legal actions to protect consumer privacy and avoid identity theft. For instance, when an online retailer of children's education materials announced that it would cease operations and sell off its assets, Pennsylvania, along with a majority of other states, filed an Objection in the Bankruptcy Court to prevent that company from selling its customer list as an asset. Ultimately, through the efforts of Pennsylvania, the FTC and 42 other states, this company agreed to destroy the customer list.

In another case where the Bureau took action against a Bucks County based national seller of computers, the Office made certain that the settlement prohibited the sale or other disclosure of customer information.

In another legal action, this Office reached an Assurance of Voluntary Compliance with a Bucks County developer and distributor of computer games to resolve alleged violations related to the company's use of "spyware" in its computer games. Customers who purchased the product were unaware that the games included a computer file attachment which allowed third party advertisers to secretly interact with the consumers' computers and trace their steps on the Internet. Asserting that this conduct violated consumer privacy rights, the Commonwealth secured an agreement from the business barring the inclusion of such programs in its products and requiring the company to provide a means for customers to remove the software program from previously purchased products.

Once again, thank you for the opportunity to comment today on the Bureau of Consumer Protection's efforts to assist consumers in preventing the growing problem of identity theft and I want to commend Congress for its recent enactment of

the Fair and Accurate Credit Transactions Act which should further assist consumers in combating this problem.

I would be happy to take any questions.

Mr. GREENWOOD. Thank you. Lieutenant Colonel Periandi.

TESTIMONY OF LT. COL. RALPH M. PERIANDI

Mr. PERIANDI. Good morning, Chairman Greenwood. I am Lieutenant Colonel Ralph Periandi, Deputy Commissioner of Operations for the Pennsylvania State Police. On behalf of Colonel Jeffrey B. Miller, Commissioner of the Pennsylvania State Police, I would like to thank the House Energy and Commerce Subcommittee on Oversight and Investigations for this opportunity to speak on the issue of identity theft.

Identity theft is delineated in Title 18, Pennsylvania Crimes Code, Section 4120. This statute indicates a person commits the offense of identity theft of another person if he possesses or uses, through any means, identifying information of another person without consent of that person to further any unlawful purpose. The unlawful activity could involve a criminal utilizing a victim's information in order to obtain access to loans, credit, or debit cards, bank accounts, services such as telephone or cable, or personal property ranging from groceries to automobiles. Following the tragic events of September 11, 2001, law enforcement must also consider the use of another person's identifying information by criminals or terrorists in an attempt to gain access to restricted areas, information—restricted areas or information in order to further their criminal enterprise.

In recent years, the crime of identity theft has grown in scope with the advent of the inexpensive personal computer. Those criminals possessing familiarity with computers now have powerful resources at their disposal. By obtaining personal, biographical and financial information which is readily available on the Internet, an identity thief can pose as anyone. Additionally, by utilizing the wide range of high quality computer peripherals, they are able to craft documents and identification which allow them to create new identities or steal the identity of someone else. Another computer aided method of committing identity theft is known as skimming. Skimming is the practice of reading and storing the magnetic information on a debit or credit card. It is easily accomplished by those in the service or retail industry by swiping a provided credit or debit card through a second card reader at the time of a legitimate transaction. The stored information is then used by that individual or sold to others for criminal purposes.

Conversely, the technologically challenged identity thief continues to resort to time tested low-tech methods for obtaining the personal information of a victim. Stealing mail, digging through garbage, generally provides the criminal with extensive personal information, to include the victim's full name, date of birth, Social Security number, bank account information, utilities account information, address and telephone number. Armed with this knowledge, the identity thief is ready to apply for credit or access funds in the name of the victim.

Currently, the best source for documented statistical information concerning the problem of identity theft, and it has previously been

testified to, is the Federal Trade Commission. The FTC has been maintaining data and information regarding this crime since enactment of the Identity Theft and Assumption Deterrence Act. In furtherance of this Act, the FTC developed the Identity Theft Data Clearinghouse and its reporting vehicle, the Consumer Sentinel. To quantify the problem of identity theft, the following information is provided from the Consumer Sentinel.

Of over 380,000 fraud complaints received nationally in 2002, the largest category of complaint was identity theft at 43 percent. Individual victim costs per fraud is estimated at $2,000. This, Mr. Chairman, the next area, national reporting of identity theft has steadily increased since the year 2000, I think you are going to find to be staggering. In 2000, which represents the first full year of reporting, slightly over 31,000 reports were received. 2001, slightly over 86,000 reports were received. This increase indicates a 177 percent change from 2000 to 2001. In 2002, almost 162,000 reports were received. Actually, 161,819, which represents an 88 percent increase over 2001. So from 2000 to 2001, we have a 177 percent increase. From 2001 to 2002, we have an additional 88 percent increase.

In the year 2002, 75 percent of victims were between the ages of 18 and 49. Of a little over 13,000 fraud complaints received in Pennsylvania during 2002, again, as is reflected nationally, the largest category of complaint was identity theft. In Pennsylvania, it amounted to 39 percent of all complaints. In 2002, Pennsylvania ranked 22nd among the states for victims of identity theft per 100,000 population, with approximately 5,080 victims.

Mr. Abel, representing the Pennsylvania Attorney General's Office, has previously testified to related statistics to these. The top three crimes committed in concert with identity theft in Pennsylvania during 2002 were credit card fraud, 46 percent of those complaints, phone or utilities fraud, 22 percent of the complaints and bank fraud, 12 percent.

The top three victim locations for identity theft in 2002 in Pennsylvania were Philadelphia, with 24 percent of the complaints, Pittsburgh, with 5 percent and Allentown, with 1 percent. Continuing in an effort to quantity this problems since the inception of the Pennsylvania statute regarding identity theft in 2001, Pennsylvania State Police have received 714 complaints involving this crime. 302 were received in the year 2001, while 412 were received in the year 2002. This represents a 27 percent increase in the number of complaints we have received in the State Police, and I think it should be noted that we are responsible for 80 percent, we are responsible for policing 80 percent of the land mass in the state, but 30 percent of the population, so a full 70 percent of the population is not reflected in the statistics regarding the complaints received by our department.

This data provides a general overview of the raw, cold, statistical information regarding the crime of identity theft. What it does not provide is insight into the associated emotional problems victims of the crime encounter. Many individuals do not discover they are the victim of an identity theft for months, if not years. Some victims have been duped for as long as 5 years. Upon discovery, victims must spend significant amounts of time contacting creditors and

credit reporting agencies in an attempt to repair the damage to their credit histories. While this is occurring, they are often unable to obtain credit and financial services, telecommunication, utility services and even employment.

Many victims report having wages garnished and tax refunds withheld. In those instances when an identity theft—an identity thief has received a criminal record in the victim's name, victims have reported having licenses revoked, family background checks and even being arrested or detained. Combating the crime of identity theft in Pennsylvania requires law enforcement to achieve three main objectives. First, law enforcement personnel must be properly trained and informed regarding this crime. Second, they must be appropriately staffed with criminal investigators to conduct these sometimes in-depth and lengthy investigations. Finally, the public needs to be provided with information concerning methods to protect themselves from identity theft, as well as information regarding the steps to take should they become a victim.

Each of these objectives will be explored more fully. In Pennsylvania, the State Police are tasked with providing police services to those areas and citizens who find themselves without their own police department. We are a full service department, performing functions ranging from traffic enforcement to criminal investigations. Our criminal investigators are responsible for the investigation of all types of crime. As such, our investigators must receive training and obtain expertise in all facets of criminal investigation. Training specific to identity theft and fraud is available to them and Pennsylvania's law enforcement community through numerous sources. Some examples are at our own Academy, Pennsylvania State Police Academy in Hershey and our regional training centers; at the Middle Atlantic Great Lakes Organized Crime Law Enforcement Network, or MAGLOCLEN, which is headquartered right here in Bucks County; the National White Collar Crime Center; International Association of Financial Crimes Investigators; the United States Department of Justice. The FTC has been previously testified to, and local banking institutions.

Generally, individual instances of identity theft are investigated by a criminal investigator assigned to one of our troop commands In those instances when a case of identity theft is indicative of organized criminal activity, the Pennsylvania State Police rely on the Organized Crime Division of our Bureau of Criminal Investigation. Members of this specially selected group of investigators are strategically located in task forces throughout Pennsylvania. They work with their troop counterparts as well as local and Federal investigators on cases involving large monetary losses, which are usually associated with organized groups of criminals.

These groups may be associated with traditional organized crime, displaced ethnic groups, or simply enterprising local criminals. Identity theft is increasingly becoming an international crime, with roots in Canada, Eastern Europe, Asia and Africa. This has made prosecution difficult, and in some cases, impossible, even with the involvement of Federal law enforcement.

In an attempt to deter or mitigate the crime of identity theft, the Pennsylvania State Police provide the following information to law enforcement agencies and the general public, and I do this, Mr.

Chairman, at the risk of repeating previous recommendations, because I think we all believe it is very important that we get this information to the public.

Let us answer a few questions for our citizens. First, how do I protect myself? These and other protective measures will not absolutely guarantee you will never become a victim of identity theft, but employing one or more of these can drastically reduce your risk.

Give your Social Security number only when it is absolutely necessary and do not carry your Social Security card with you. Leave it at home or in a secure place. Annually, review your Social Security personal earnings and benefits statement, which is mailed to all participants. A copy can also be requested from the Social Security Administration. Memorize your ATM password and shield the keypad when entering your password at any ATM machines. Previously, Mr. Chairman, I believe you asked a question relative to passwords and PIN numbers particularly. And we have had instances where criminals from a remote location will videotape the keypad and then, by certainly expanding or utilizing that videotape to basically just look at the particular PIN information, and they have already captured possibly your password information or your account number information.

Do not place bill payments in your mailbox for pickup. We saw that in one of the videos. Mail your bills directly from the Post Office. Shredding of documents, which we have already talked about. Annually obtaining your credit report from the three major credit reporting agencies. Carefully review them for accuracy and immediately correct all mistakes. Have your name removed from lists sold to companies offering pre-approved credit cards. That has already been testified to and questioned and discussed, by contacting three credit card reporting agencies.

Do not give your credit card number over the telephone unless you have initiated the call. Ensure that neither you nor the called party is using a mobile or cellular telephone. This is another issue that we deal with where people speak freely on mobile phones and cellular telephones without regard for the fact that that can often be intercepted. When you purchase items with a credit card, take your receipts with you. Do not toss them away. Do not put your credit card number on the Internet unless it is an encrypted or secured site.

How about the question what if I become a victim of identity theft? Identity theft can occur even if you have been careful about protecting your personal information because of the ever-increasing skill employed by professional thieves. The exact steps that you should take after becoming a victim of identity theft will vary depending upon your circumstances, but in most instances, the following steps should be taken.

Mr. GREENWOOD. I am going to ask you to just kind of go through these steps real——

Mr. PERIANDI. Skip through those?

Mr. GREENWOOD. Real quickly, and—because——

Mr. PERIANDI. Okay. Contact the security department of the respective financial institution. Contact each of the Nation's credit reporting agencies. File a complaint with your local police depart-

ment or law enforcement agency where the identity theft took place, and I know previously Mrs. Kane talked about the problem relative to jurisdiction and venue. That has been cleared up with an amendment in 2002 in Pennsylvania, so that prosecution can be taken at either the residence or the work location of the victim.

Report fraudulent use of your Social Security number to the Social Security Administration. Notify the United States Postal Service, which has been testified to, and notify immediately your agency, if an ATM card has been lost or stolen or any of that information has been compromised.

Same thing with checks. If you are a victim of identity theft, never agree to pay any portion of the debt just to get a collection agency off the case. The Fair Debt Collection Act prohibits collectors from contacting you if within 30 days after you receive their written notice, you send them a letter refuting the debt, et cetera, with supporting documentation relative to criminal violation.

Unfortunately, it is impossible to protect yourself entirely from identity theft, but following the safeguards detailed herein can greatly reduce your risk.

Additionally, the Pennsylvania State Police provides numerous other services to Pennsylvania citizenry and law enforcement community in dealing with the problem of identity theft. The Bureau of Forensic Services offers examination of questioned documents, handwriting comparisons, patent and latent fingerprint identification comparison. The Polygraph Unit in many instances is required to determine the veracity of involved suspects. Community Services Unit performs speeches and provides information to community groups concerning how to reduce the probability of becoming a victim of this type of theft. The Bureau of Criminal Investigation, through the Department's Pennsylvania Criminal Intelligence Center, or PaCIC, provides briefs, which contain information concerning prevention and response methods for crimes such as identity theft. In addition, ongoing analysis of data helps PaCIC to identity trends in an effort to alert law enforcement statewide to potential organized efforts to commit identity theft.

Finally, with the advent and ease of access to computer technology, the State Police Area Computer Crime Task Forces have become an invaluable resource to Pennsylvania law enforcement, particularly in those instances when a computer has been utilized in some way to steal an individual's identity or commit a crime utilizing another's identity.

As you can see, Mr. Chairman, the Pennsylvania State Police brings a wide variety of investigative resources to combat the evolving problem of identity theft in the Commonwealth. Through experience, we have learned to utilize and share these resources with local, State and Federal investigators. Only by sharing resources and staying ahead of the criminal mind will we be effective in this crime fighting effort.

Finally, recent legislative changes to Pennsylvania's identity theft statute have made investigation and prosecution for this crime a more efficient and effective process. I mentioned the fact that the venue has been changed and penalties have been enhanced. The clarification of venue is particularly important, as

many of the crimes associated with identity theft occur in other jurisdictions, states and countries.

In closing, I would like to thank Chairman Greenwood and the Members of the committee for the opportunity to address you today on this issue. As a member of the Pennsylvania State Police, each officer carries on a tradition of excellence begun in the year 1905. As part of this tradition, it is the mission of each member of our department to effectively investigate crime and criminal activity, provide investigative assistance and support to all law enforcement within the Commonwealth, and promote public awareness concerning personal responsibility regarding crime reduction. This includes the crime of identity theft.

I welcome the opportunity to respond to any questions or comments you may have.

[The prepared statement of Ralph M. Periandi follows:]

PREPARED STATEMENT OF LT. COL. RALPH M. PERIANDI, DEPUTY COMMISSIONER OF OPERATIONS, PENNSYLVANIA STATE POLICE

Good morning Mr. Chairman and members of the Committee. I am Lt. Col. Ralph M. Periandi, Deputy Commissioner of Operations for the Pennsylvania State Police. On behalf of Colonel Jeffrey B. Miller, Commissioner of the Pennsylvania State Police, I would like to thank the House Energy and Commerce Committee for this opportunity today to speak on the issue of Identity Theft.

Identity Theft is delineated in Title 18, the Pennsylvania Crimes Code, Section 4120. This statute indicates a person commits the offense of identity theft of another person if he possesses or uses, through any means, identifying information of another person without consent of that other person to further any unlawful purpose. The unlawful activity could involve a criminal utilizing a victim's personal information in order to obtain access to loans, credit or debit cards, bank accounts, services such as telephone or cable, or personal property ranging from groceries to automobiles. Following the tragic events of September 11, 2001, law enforcement must also consider the use of another persons identifying information by criminals or terrorists in an attempt to gain access to restricted areas/information in order to further their criminal enterprise.

In recent years, the crime of Identity Theft has grown in scope with the advent of the inexpensive personal computer. Those criminals possessing familiarity with computers now have powerful resources at their disposal. By obtaining personal biographical and financial information, which is readily available on the Internet, an identity thief can pose as anyone. Additionally, by utilizing the wide range of high quality computer peripherals available, they are able to craft documents and identification, which allow them to create new identities or steal the identity of someone else. Another computer aided method of committing Identity Theft is known as "skimming". "Skimming" is the practice of reading and storing the magnetic information on a debit or credit card. It is easily accomplished by those in the service or retail industry by "swiping" a provided credit or debit card through a second card reader at the time of a legitimate transaction. The stored information is then used by that individual or sold to others for criminal purposes.

Conversely, the technologically challenged identity thief continues to resort to time tested low-tech methods for obtaining the personal information of a victim. Stealing mail and digging through garbage generally provides the criminal with extensive personal information to include the victim's full name, date of birth, social security number, bank account information, utilities account information, address, and telephone number. Armed with this knowledge, the identity thief is ready to apply for credit or access funds in the name of the victim.

Currently, the best source for documented statistical information concerning the problem of Identity Theft is the Federal Trade Commission (FTC). The FTC has been maintaining data and information regarding this crime since enactment of the Identity Theft and Assumption Deterrence Act in 1998. (Pub. L. No. 105-318, 112 Stat. 3007) In furtherance of this Act, the FTC developed the Identity Theft Data Clearinghouse and its reporting vehicle, the Consumer Sentinel. To quantify the problem of identity theft, the following information is provided from the Consumer Sentinel:

- Of 380,103 fraud complaints received nationally in 2002, the largest category of complaint was Identity theft at 43%.
- The Financial costs to victims of all fraud reported in the nation during the year 2002 is estimated at nearly ½ billion dollars. 43% of this figure would indicate Identity Theft nationwide cost victims approximately $200 Million.
- Individual victim cost per fraud is estimated at $2,000.
- National reporting of Identity Theft has steadily increased since the year 2000. In 2000, which represents the first full year of reporting, 31,117 reports were received. During 2001, 86,198 reports were received. This increase indicates a 177% change over the previous year. Finally, in 2002, 161,819 reports were received, which represents an 88% increase over the year 2001.
- In the year 2002, 75% of victims were between the ages of 18-49.
- Of 13,119 fraud complaints received in Pennsylvania during 2002, the largest category of complaint was Identity theft at 39% of all complaints.
- In 2002, Pennsylvania ranked 22nd among states for victims of Identity Theft per 100,000 population, with 5,080 victims.
- The top three crimes committed in concert with an Identity Theft in Pennsylvania during 2002 were Credit Card Fraud with 2,359 victims (46%), Phone or Utilities Fraud with 1,103 victims (22%), and Bank Fraud with 623 victims (12%).
- The top three victim locations for Identity Theft in 2002 were Philadelphia with 1,202 victims (24%), Pittsburgh with 226 victims (5%), and Allentown with 70 victims (1%).

Continuing, in an effort to quantify this problem since the inception of the Pennsylvania statute regarding Identity Theft in 2001, the Pennsylvania State Police have received 714 complaints involving this crime. 302 were received in the year 2001, while 412 were received in 2002. This represents a 27% increase.

This data provides a general overview of the raw, cold statistical information regarding the crime of Identity Theft. What it does not provide is insight into the associated emotional problems victims of this crime encounter. Many individuals do not discover they are the victim of Identity Theft for months, if not years. Some victims have been duped for as long as five years. Upon discovery, victims must spend significant amounts of time contacting creditors and credit reporting agencies in an attempt to repair the damage to their credit histories. While this is occurring, they are often unable to obtain credit and financial services, telecommunication and utility services, and even employment. Many victims report having wages garnished and tax refunds withheld. In those instances when an identity thief has received a criminal record in the victim's name, victims have reported having licenses revoked, failing background checks, and even being arrested or detained.

Combating the crime of Identity Theft in Pennsylvania requires law enforcement to achieve three main objectives. First, law enforcement personnel must be properly trained and informed regarding this crime. Second, they must be appropriately staffed with criminal investigators to conduct these sometimes in-depth and lengthy investigations. Finally, the public needs to be provided with information concerning methods to protect themselves from Identity Theft, as well as information regarding the steps to take should they become a victim. Each of these objectives will be explored more fully.

In Pennsylvania, the State Police are tasked with providing police services to those areas and citizens, who find themselves without their own police department. We are a full service department, performing functions ranging from traffic enforcement to criminal investigations. Our criminal investigators are responsible for the investigation of all types of crime. As such, our investigators must receive training and obtain expertise in all facets of criminal investigations. Training specific to Identity Theft and fraud is available to them and Pennsylvania's law enforcement community through numerous sources. Some examples are: the Pennsylvania State Police Academy; the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN); the National White Collar Crime Center (NW3C); the International Association of Financial Crimes Investigators; the U.S. Department of Justice; and local banking institutions.

Generally, individual instances of Identity Theft are investigated by a Criminal Investigator assigned to one of our Troop commands. In those instances when a case of Identity Theft is indicative of organized criminal activity, the Pennsylvania State Police rely upon the Organized Crime Division of the Bureau of Criminal Investigation. Members of this specially selected group of investigators are strategically located in task forces throughout Pennsylvania. They work with their Troop counterparts, as well as local and federal investigators on cases involving large monetary losses, which are usually associated with organized groups of criminals. These groups may be associated with traditional organized crime, displaced ethnic groups, or simply enterprising local criminals. Identity Theft is increasingly becoming an

international crime with roots in Canada, Eastern Europe, Asia and Africa. This has made prosecution difficult and in some cases impossible even with the involvement of federal law enforcement agencies.

In an attempt to deter or mitigate the crime of Identity Theft, the Pennsylvania State Police provide the following information to law enforcement agencies and the general public:

How Do I Protect Myself?

These and other protective measures will not absolutely guarantee you will never become a victim of Identity Theft, but employing one or more of these can drastically reduce your risk:

- Give your social security number only when it is absolutely necessary, and do not carry your social security card with you. Leave it at home or in a secure place.
- Annually review your social security personal earnings and benefit statement which is mailed to all participants. A copy can also be requested from the Social Security Administration (1.800.772.1213).
- Memorize your ATM password and shield the keypad when entering your password at ATM machines.
- Do not place bill payments in your mailbox for pickup. Mail your bills directly from the post office.
- Shred all documents containing personal information especially bills, credit card receipts, pre-approved credit card offers, and bank statements, before you throw them away.
- Annually obtain a copy of your credit report from the three major credit reporting agencies (Trans Union, 1.800.680.7289) (Equifax, 1.888.766.0008) (Experian, 1.888.397.3742). A basic report costs $9.00 from any of the three agencies. Certain states have passed legislation giving residents free or reduced prices on credit reports. Carefully review them for accuracy and immediately correct all mistakes identified on your credit reports in writing.
- Have your name removed from lists sold to companies offering preapproved credit cards by contacting the three credit reporting agencies and taking advantage of their "optout" service. One number, 1.888.567.8688, reaches all three agencies.
- Do not give your credit card number over the telephone unless you have initiated the call. Ensure that neither you nor the called party is using a mobile or cellular telephone.
- When you purchase items with a credit card, take your receipts with you, do not toss them away.
- Do not put your credit card number on the Internet unless it is an encrypted or secured site.

What If I Become A Victim of Identity Theft?

Identity Theft can occur even if you have been careful about protecting your personal information because of the ever-increasing skill employed by professional thieves. The exact steps that you should take after becoming a victim of Identity Theft will vary depending upon your circumstances, but in most instances, the following steps should be taken:

- Contact the security department of the respective financial institution, both verbally and in writing, for each account that has been opened or tampered with and close these accounts. The federal Fair Credit Billing Act limits your liability for unauthorized charges to $50.00, but it's your responsibility to make the appropriate notification, in writing, within 60 days after the fraudulent activity has been discovered. Once the financial institution acknowledges the fraud, ask them to send all three credit reporting agencies a letter confirming fraudulent activity.
- In the past, one necessary step included contact with each of the nation's three major credit reporting agencies (TransUnion, Equifax, and Experian). In an effort to streamline the process, the credit reporting agencies have agreed to begin sharing fraud related information. As of April 15, 2003, Identity Theft victims need only make one toll-free call to any of the three nationwide credit reporting agencies. The information they provide will be automatically shared with the remaining agencies for inclusion in their records. Within 24 hours of being notified, each credit reporting agency will post a security alert on the victim's credit file, which will be viewed by all lenders or other users accessing future reports. The alert will notify lenders of the reported fraud, thereby assisting them to avoid opening a fraudulent account in the victim's name. The credit reporting agencies will also remove the victim's name from the lists of pre-approved credit or insurance offers for a period of two years. Additionally, the agencies have agreed to provide each victim with a copy of his or her credit file,

and to simplify the information verification process to include deletion of fraudulent information.

- File a complaint with your local police department or the law enforcement agency where the Identity Theft took place. Also, file a complaint with the Federal Trade Commission (FTC) Identity Theft Hotline by telephone at 1.877.IDTHEFT. Although the FTC has no criminal law enforcement authority, they can pursue civil remedies and assist victims in resolving the problems associated with the crime.
- Report the fraudulent use of your social security number to the United States Social Security Administration at 1.800.269.0271. Under certain circumstances, a new social security number may be issued.
- Notify your nearest United States Postal Inspection Service if you suspect the theft of your mail.
- If your ATM card has been lost or if your password has been compromised, immediately notify your bank. The Electronic Fund Transfer Act limits your losses to $50.00 if you make this report within two business days. If you wait more than 60 days to make the report, you could lose all the money that was taken from your account.
- If checks were stolen or fraudulent bank accounts were established, report this to your bank and to the major check verification companies (Telecheck, 1.800.710.9898) (Certegy Inc., 1.800.437.5120) (International Check Services, 1.800.631.9656). Request they notify retailers who use their service that you were the victim of Identity Theft.
- If you're a victim of Identity Theft, never agree to pay any portion of the debt just to get collection agencies off the case. The Fair Debt Collection Act prohibits collectors from contacting you if within 30 days after you receive their written notice, you send them a letter refuting the debt. Along with your letter, send supporting documentation (police report, letters from credit reporting agencies, etc.) to substantiate your position.

Unfortunately, it is impossible to protect yourself entirely from Identity Theft, but following the safeguards detailed herein can certainly reduce your risk. Publications by the Federal Trade Commission (FTC) can provide further information on how to prevent Identity Theft. These publications can be obtained by contacting the FTC by telephone at 1-877-IDTHEFT or by visiting their web sites at http://www.ftc.gov or at http://www.consumer.gov. Phone counselors at the FTC can assist callers on how to take advantage of their consumer rights and on what actions need to be taken to restore their credit.

Additionally, The Pennsylvania State Police provides numerous other services to Pennsylvania's citizenry and law enforcement community in dealing with the problem of Identity Theft. The Bureau of Forensic Services offers examination of questioned documents, handwriting comparisons, and patent and latent fingerprint identification and comparison. The Polygraph Unit in many instances is required to determine the veracity of involved suspects. The Community Services Unit performs speeches and provides information to community groups concerning how to reduce the probability of becoming a victim of this type of crime. The Bureau of Criminal Investigation through the Department's "Pennsylvania Criminal Intelligence Center" (PaCIC), provides Briefs, which contain information concerning prevention and response methods for crimes such as Identity Theft. In addition, ongoing analysis of data helps PaCIC to identify trends in an effort to alert law enforcement statewide to potential organized efforts to commit Identity Theft. Finally, with the advent and ease of access to computer technology, the State Police Area Computer Crime Task Forces have become an invaluable resource to Pennsylvania law enforcement, particularly in those instances when a computer has been utilized in some way to steal an individual's identity or commit a crime utilizing another's identity.

As you can see, the Pennsylvania State Police brings a wide variety of investigative resources to combat the evolving problem of Identity Theft in the Commonwealth. Through experience, we have learned to utilize and share these resources with local, state and federal investigators. Only by sharing resources and staying ahead of the criminal mind will we be effective in this crime fighting effort.

Finally, recent legislative changes to Pennsylvania's Identity Theft statute have made investigation and prosecution for this crime a more efficient and effective process. Penalties have been stiffened and venue now includes the residence or employment address of the person whose identifying information has been lost or stolen or has been used without the person's consent. The clarification of venue is particularly important as many of the crimes associated with Identity Theft occur in other jurisdictions, states, or countries.

In closing, I would like to thank the Chairman and members of the Committee for the opportunity to address you today on this issue. As a member of the Pennsylvania State Police, each officer carries on a tradition of excellence begun in the year 1905. As part of this tradition, it is the mission of each member to effectively investigate crime and criminal activity, provide investigative assistance and support to ALL law enforcement agencies within the Commonwealth, and promote public awareness concerning personal responsibility regarding crime reduction. This includes the crime of Identity Theft. I welcome the opportunity to respond to any questions or comments you may have.

Mr. GREENWOOD. Thank you, sir. I appreciate it. Let me go back to the tape we saw with Mr. Lomax, if that is, in fact, his real name. Walked through how easy it was for him to steal actor Will Smith's identity. He basically looked in a magazine that probably had an article that said who his mother and his mother's maiden name, what his mother's maiden name was, address and enough identifying information gleaned from a source like that to then go, and what he said he did, as I recall, was to go and get, first off, a duplicate birth certificate, and then take that and get a duplicate Social Security card, and then take that and get a duplicate driver's license. The question I have for any or all of you. If Mr. Lomax gets out of jail tomorrow, and wants to start all over again, picking another victim, would he be able to do it just as easily today as he did initially? Anything changed that makes his job more difficult?

Mr. BURKE. Well, sir, I would like to believe no. One of the——

Mr. GREENWOOD. Pull the microphone close to you.

Mr. BURKE. One of the—he mentioned mother's maiden name. I will give you an example. The Inspection Service, in concert with the banking industry, meets, they have an initiative, it is the Financial Crimes Mail Security Initiative, and we meet twice a year, and at those meetings, we discuss best practices. The young lady from the bank in Newtown mentioned the—as an example, the 1-800 number, and then of course, Mr. Lomax, I believe that is his real name, mentioned the mother's maiden name. Well, the 1-800 sticker that you now get on your credit cards was a result of an Inspection Service initiative, and in particularly, a now retired Inspector working out of Florida, and as odd as this may seem, in developing this 1-800 number and asking for pertinent information that only the individual would know, someone suggested at one of these meetings that they use the mother's maiden name. Well, lo and behold, it became an industry standard. Now, the good news is that they are varying that. They are asking other pertinent information. So that is an example of how it is becoming more difficult.

And as was mentioned several times here today, the interaction with State and local, Federal law enforcement now, and the publicity due in large part because of committees and meetings and public referendums like this is doing a great deal of good to prepare people for it.

In the past, local law enforcement may take a complaint on a credit card and quite honestly, it was difficult for them to give it the time and effort it needed, because it crossed jurisdictional lines. Now, with the FTC downloading the data and everything and everyone having access to that, we have minimized that, too, so I think through educating the public and the aggressive interaction across the board from law enforcement at every law, there are

more and more stopgaps that are being put in that will make it more and more difficult.

Mr. GREENWOOD. You may share the microphone with Ms. Broder.

Ms. BRODER. I guess I can't say with real confidence that it would be that much more difficult to accomplish what Mr. Lomax did if he gets out of jail tomorrow. But one of the new provisions of the FACT Act requires the FTC, along with the bank regulatory agencies to develop guidelines for red flags, that is the pattern, what are the indicia of fraud, and when we see these types of patterns emerging, what should be done? He talked about 17 to 18 accounts opened in a short period of time. Mrs. Kane referred to a 33 page credit report for someone who had a very normal pattern before. So the question is what can the financial agencies do to pinpoint that where now they are not, where they are not aware of the fraud, they are not paying attention to those as closely as they might.

Mr. PERIANDI. Mr. Chairman.

Mr. GREENWOOD. What about the—go ahead, yes, please, Colonel.

Mr. PERIANDI. If I could add. Unfortunately, your question is right on point. But it goes to something that we have found even in the area of terrorism, and that is, it goes to the identifying documents, the base documents. When someone has a birth certificate, Social Security card and driver's license that appears to be legitimate, and is in fact legitimate, because it has been obtained from legitimate agencies, it makes it very, very difficult for law enforcement. I won't comment for the private sector, but it makes it very, very difficult for law enforcement to work through that and identity this individual as being a criminal, because all the documents, the supporting documentation that you would look at is accurate.

They have a reliable and accurate birth certificate. They have a reliable and accurate driver's license, particularly which is a photo identification, so I can only assume that when they present this at a retail establishment, or even within the banking industry, that that information is going to be accepted, and that—so it gets, I think you make a very good point. We need to look at how easy it is for criminals to obtain that identifying documentation that really gives them access to the rest of the system. Once they have that documentation, they have access to the rest of the system.

Mr. GREENWOOD. And of course, the tricky part in this is that any of us can lose our driver's license or Social Security card, or for that matter, our birth certificate, and want to get copies of it, and so we don't want the government to make it impossible or extraordinarily difficult. Sometimes, we might need those documents in a hurry, like for travel or something like that, and so it is a tough balance. Let me talk—ask about the consequences on the other side of this quotient. We have—I think the Postal Inspection Service talked about 3,000 arrests in a year. One of the things that seems to make a difference in criminal conduct is when someone says—when people are talking, potential criminals, criminal are talking amongst themselves, they say I went to jail, or I did hard time, or you know, I got off easy.

When we make all these arrests, are we in fact coming down hard enough on the perpetrators in terms of are they—do we have the—are we—sometimes, I see that in law enforcement—is given limited resources and time and money. It is only the biggest cases that are actually taken in to prosecution and the smaller cases are disposed of in some other way, probationary response. There is not even always restitution, so it is a—who would like to comment on how effective we are being in various law enforcement agencies in actually making sure that people pay consequences for these crimes?

Mr. BURKE. Congressman, I think that—I think we are starting to see a change in the trends, but as is often the case in local prosecutor, State and Federal prosecution, they have quite a lot on their table, and oftentimes, they will put dollar restrictions or dollar limitations that a case would have to be over, say, $50,000 for it to be accepted for prosecution, and that varies, and of course, each case stands in and of itself. From an investigator's standpoint, certainly you are not going to get to me to say that every perpetrator that commits identity theft, or any crime for that matter, gets a fair and just sentence, because certainly as investigators, we would like to see them get as much as possible.

Oftentimes, some of the groups, as was mentioned by the State Police, are organized ethnic groups, and then you are dealing with Federal entities like the INS and all, and you can identify these people, and quite honestly, sometimes, they are deported and back several years later. You run into them again. So, I think we can go a long way to come up with uniform sentencing guidelines. Certainly, there is, in the Federal Government sentencing guidelines, but they are not always applied equally, because of the size of the case and other considerations.

Mr. GREENWOOD. Anyone else wish to comment on that?

Mr. PERIANDI. I would say I tend to agree, if we take Mrs. Kane's example, an individual who perpetuates an identity theft generally is perpetuating it on numerous individuals, so it makes sense to prosecute that individual where they are located. In her case, it was in Schenectady, New York. However, I think we recognize that if that individual would have been extradited to Bucks County and tried here, where the victim resides, and where the victim would be identified, or the judges and the court system would identify with the victim, the probability for a stronger, harsher sentence and to actually server that stronger, harsher sentence is increased. So, we really need to work between the states to ensure that when that case is prosecuted in Schenectady, New York, that somehow, we drive home the same kind of identity with the victim and the emotions associated with what would happen if that individual were tried here in Bucks County, and I think it does come to some type of standard sentencing, but you know, I don't know how you do that in 50 individual states without impacting states' rights issues from the Federal level.

Mr. GREENWOOD. Ms. Kane talked about the fact that the people prosecuting the case really didn't stay much in touch with her, that the banks had experienced the actual financial losses, so they hired an investigator, and then they gave that information to law enforcement, but that she was pretty much out of the loop and didn't

have the opportunity to ever to confront the woman who had defrauded her, or to observe the trial, testify at the trial. What is the state-of-the-art today? Are we seeing your agencies, those of you particularly in the criminal side of this thing, actually staying and recognizing that the victim is not just the finance institution but the person whose identity has been stolen and keeping in touch with that person, or keeping them in the loop?

Mr. PERIANDI. We try to, Mr. Chairman, but that really is a function of the prosecutor's office, and what we have found, particularly if the prosecutor is in touch with the victim, at least specifically during the sentencing stage, that that is very helpful to have the victim present and able to testify prior to sentencing, or just say a few words to the Court prior to sentencing. But we certainly will reach out to victims when the case proceeds to that particular point, as long as we are notified, again, by the prosecutor's office, but that really becomes their function at that point.

Mr. GREENWOOD. Ms. Broder, let me ask you, much has been mentioned of the FACT Act today. Does the FTC feel that the U.S. Congress has completed its work on identity theft, or is there more to do?

Ms. BRODER. Well, in light of the 18 rulemaking, studies and reports, we think they have done enough for the time being. This is—it has been a dramatic change through the FACT Act, and substantial changes will take place in the financial industries as well, and I think this, speaking for myself here, is the right step, and then we see what effect these changes have on the incidence of identity theft and the recovery of victims, and if this is not adequate, I think it is time to go back to the drawing board, but for the time being, it seems like a very comprehensive approach to the problem, sir.

Mr. GREENWOOD. Congress has given you a lot of work to do. Has Congress given you enough resources to do it?

Ms. BRODER. I think we are well prepared to take on these tasks, Mr. Chairman. Part of our program is to leverage our resources so that we make our resources available to others. That is the whole idea behind the training of local law enforcement. Let them convey our message as well. We do that also through the credit reporting agencies and the financial institutions. We make all of our publications available on a CD-ROM, English and Spanish, the books, the affidavit, so that other agencies, banks, can print them as well, put their names on the front cover. We don't care, as long as they get the message out. So for the time being, I think we are okay. Thank you very much.

Mr. GREENWOOD. The—when we heard about the Red Cross and the folks using the information on blood supplies, I though that was about as low as it could go, until we learned about the Medical Examiner's employees gleaning information from dead bodies. How did the perpetrators achieve that crime, accomplish that crime?

Mr. BURKE. Well, they—the pedigree of the information they got, actually, from my understanding, is the credit card from the deceased, and then once they had that——

Mr. GREENWOOD. So they actually go through the wallets of——

Mr. BURKE. They go through the personal belongings of the deceased, and of course, once you have that basic data, then you can build your fraudulent activity from there.

Mr. GREENWOOD. That is as low as you can go.

Mr. BURKE. I would say it is, sir.

Mr. GREENWOOD. You also talked in your testimony, Mr. Burke, about individuals purchasing commercial grade credit card embossing machines over the Internet. Is anyone looking at—there are so many purchases you can make over the Internet now, of a very illegal nature, and at least—ways to access all kinds of tools for committing crimes, and this is the latest one that I have heard of. Is anyone taking action to try to limit the access, the availability of this equipment?

Mr. BURKE. Not—certainly not the Inspection Service. What I have here, Congressman, is a copy of—one of our Inspectors downloaded this. This is the same website, and there is an embosser there, so I can give it to your——

Mr. GREENWOOD. Okay. Well, the staff will pick that up after the hearing. And I think that is something that should be pursued. It would be interesting to know whether the actual manufacturers are marketing their products this way, and why they would do that. Maybe they have a perfectly legitimate reason, but it seems that that is the kind of equipment that is very dangerous, obviously, in the hands of the wrong individuals, and we need to be careful with that. Let me just see if I have another kind of question that needs to be asked. Well, I think we have gone long enough, and I do thank all of the witnesses in this last panel as well as all of the witnesses throughout this hearing the last several hours. It is a big help. Our intent here is twofold, one is to use the media that is here to help inform the public in this region of the precautions that they need to take and what they should do if they are victims, and the others to see what kinds of tasks that may lay before Congress and if it is not giving more authority to the FTC, it may be pursuing issues like the availability of this kind of equipment on the Internet. So with that, I would also like to thank Ms. Washington, to my right, who as the counsel for this committee, and my staff and the District and Washington for helping this—organize this hearing, and it is now adjourned.

[Whereupon, at 1:14 p.m., the subcommittee was adjourned.]

○