FIELD HEARING ON SOCIAL SECURITY NUMBERS AND CHILD IDENTITY THEFT

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

SEPTEMBER 1, 2011

Serial 112–SS9

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE

74–006 WASHINGTON : 2011

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY

SAM JOHNSON, Texas, *Chairman*

KEVIN BRADY, Texas
PAT TIBERI, Ohio
AARON SCHOCK, Illinois
RICK BERG, North Dakota
ADRIAN SMITH, Nebraska
KENNY MARCHANT, New York

XAVIER BECERRA, California
LLOYD DOGGETT, Texas
SHELLEY BERKLEY, Nevada
FORTNEY PETE STARK, California

JON TRAUB, *Staff Director*
JANICE MAYS, *Minority Staff Director*

CONTENTS

FIELD HEARING ON SOCIAL SECURITY NUMBERS AND CHILD IDENTITY THEFT

THURSDAY, SEPTEMBER 1, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 12:00 p.m., in the Plano City Council Chamber, 1520 Avenue K, Plano, Texas, Honorable Sam Johnson [chairman of the subcommittee] presiding.

[The advisory of the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

September 01, 2011

Subcommittee on Social Security Chairman Johnson Announces Field Hearing on Social Security Numbers and Child Identity Theft

U.S. Congressman Sam Johnson (R–TX), Chairman of the House Committee on Ways and Means Subcommittee on Social Security announced today that the Subcommittee will hold a field hearing on Social Security numbers (SSNs) and child identity theft. **The hearing will take place on Thursday, September 1, 2011 in the Plano City Council Chamber, 1520 Avenue K, Plano, Texas at 12:00 p.m. Central Standard Time.**

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

BACKGROUND:

According to the U.S. Department of Justice, between 2006 and 2008, approximately 11.7 million people were victims of identity theft. The Federal Trade Commission (FTC) estimates that identity theft costs consumers about $50 billion annually. Further, identity theft is often used to facilitate other crimes, including credit card, document, or employment fraud. The Social Security number (SSN) is especially valuable to identity thieves who can use it to create a false identity in order to open accounts or obtain other benefits in the victim's name.

Perhaps more disturbing is the growing trend in child identity theft. There were 19,000 cases of child identity theft reported to the FTC in 2009, a 192 percent increase since 2003 when 6,500 cases were reported.

Family members may use a child's name and SSN to obtain new credit. Other criminals may obtain a child's name and SSN or use different names and birth dates to avoid detection as businesses granting credit may not ensure names, SSNs, or dates of birth match. In the meantime, children of all ages whose SSNs have been compromised may discover years later that they have a record of bad debt including years of unpaid bills, credit card debt, or loan defaults. Recently, the FTC has intensified its work regarding the growing problem of child identity theft, gathering identity theft experts and law enforcement officials for the first ever conference on child identity theft in July 2011 entitled, "Stolen Futures, A Forum on Child Identity Theft."

In announcing the hearing, Chairman Sam Johnson (R–TX) stated, **"Identity thieves prey on the good credit of law abiding citizens. Social Security numbers, even those belonging to children, are often the keys to pulling off these crimes. Taking steps to stop the overuse of Social Security numbers and giving law enforcement better tools to stop these thieves will help prevent identity theft and further protect the privacy of all Americans and their children."**

FOCUS OF THE HEARING:

The Subcommittee will examine the emerging patterns of child identity theft, the role of SSNs in these crimes and steps families can take to help protect themselves.

Legislative options to help prevent these crimes and assist law enforcement will also be considered.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, *http://waysandmeans.house.gov*, select "Hearings." Select the hearing for which you would like to submit, and click on the link entitled, "Click here to provide a submission for the record." Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word or WordPerfect document, in compliance with the formatting requirements listed below, **by the close of business on Thursday, September 15, 2011**. Finally, please note that due to the change in House mail policy, the U.S. Capitol Police will refuse sealed-package deliveries to all House Office Buildings. For questions, or if you encounter technical problems, please call (202) 225–1721 or (202) 225–3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any supplementary materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission or supplementary item not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All submissions and supplementary materials must be provided in Word format and MUST NOT exceed a total of 10 pages, including attachments. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

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

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

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

Chairman JOHNSON. The hearing will come to order.

Back in November 1936, the U.S. Postal Service first began issuing Social Security cards to workers. Even though Social Security numbers were created to track earnings for determining Social Security benefits, today these numbers are widely used as personal identifiers.

Some uses of Social Security numbers are mandated, for example, for income and tax-related reporting to the IRS by employers, banks and insurance companies. Countless other businesses use this nine-digit number as a default identifier to facilitate the matching of consumer information. Also, many businesses wrongly use Social Security numbers to prove an individual is who they say they are; in other words, an identification number.

Once a thief has someone's Social Security number, they're often able to open new accounts, access existing accounts or obtain other benefits in the victim's name. In fact, in their April 2007 report,

the Identity Theft Task Force created by President George Bush identified the Social Security number as the most valuable commodity for an identity thief. Months or even years later, victims first learn about the crime often after being denied credit or employment or being contacted by a debt collector.

As we will hear from two of our witnesses today, learning your private, personal and financial information has been compromised is devastating. Even worse, victims must take the lead in repairing and restoring their records.

For years victims have to prove who they are while monitoring credit reports, arguing with collection agencies and dealing with the IRS and Social Security about wages they didn't earn and taxes they don't owe. Some may learn they have a criminal record which could disqualify them for a job.

Americans are right to be concerned. According to the Department of Justice, in 2009, ID theft claimed over 11 million victims. That's 5 percent of all adults. The Privacy Rights Clearinghouse reports a total number of known records that have been compromised since 2005 through last week topped 535 million.

Increasingly, identity thieves are aiming their sights on children. There were 19,000 cases of child identity theft reported to the FTC in 2009 a 192 percent increase since 2003. From the criminal's point of view, children provide easy targets since they have no debt history and no reason to check their credit cards.

Child ID thieves may operate undetected for years until the child applies for driver's license, credit card or jobs and learns their ID has been compromised. In some very sad cases, the child is a victim of a relative. In the meantime, children of all ages whose Social Security number has been compromised may have a record of credit card debt, mortgage default or falsified employment.

As we will hear from the Director of the Federal Trade Commission, Southwest Region today, the FTC has recently intensified its work regarding the growing problem of child identity theft, gathering experts and law enforcement officials last month for the first time ever conference on child identity theft.

And we will gain some insights on the identity thieves themselves based on the research of one of our own University of Texas at Dallas professors who will share the results of her interviews conducted with ID thieves. Lastly, we will hear from the local agents from the Social Security Administration Office of the Inspector General about their successes and challenges as they work to apprehend ID theft cases.

Congress needs to finish its work on ID theft. Previously, bipartisan legislation has been passed by the Ways and Means Committee to protect the privacy of Social Security numbers and prevent identity theft. While progress has been made, because Social Security number use is so widespread, and there are several Committees of Jurisdiction, we have yet to reach agreement on the right ways to limit SSN access.

In the mean time, this Committee can make progress by removing Social Security numbers from Medicare cards. To that end, I have introduced with my Texas colleague, Lloyd Doggett, the Medicare Identity Theft Prevention Act.

The risk of ID theft goes far beyond the card being stolen. Every medical record at doctor's offices, hospitals and nursing homes has a Social Security number written on it. The fact that millions of Social Security numbers are readily available to identify thieves for the taking is kind of unbelievable.

The Centers for Medicare and Medicaid Services have refused to act; and if they won't do right for America's seniors, we will try. With the help of information gathered from our witnesses today, we can also do what's right for children and help protect them from ID theft.

I thank all of you for being here today and sharing with us the information that you have. As is customary, any member of this committee is welcome to submit an opening statement for the record; but before we move on, I want to remind our witnesses to limit their oral statements to five minutes. And without objection, all written testimony will be made part of the permanent record.

Chairman JOHNSON. We have one panel today and our witnesses who are seated at the table are: Stanley Lanius from Plano. Raise your hand.

Ms. LANIUS. Stacey.

Chairman JOHNSON. Stacey it is. Excuse me. I was looking for a guy and it's a girl. Thank you for being here, ma'am. I apologize.

Steve Bryson from Allen; and Deanya Kueckelhan, Director Southwest Region, Federal Trade Commission from Dallas; and Lynne Vieraitis, Ph.D. Associate Professor of Criminology in the University of Texas, Dallas in Richardson; Robert Feldt, Special Agent In-Charge, Office of the Inspector General, Social Security Administration, Dallas. And Mr. Feldt is accompanied by Antonio Puente, Special Agent from the Dallas Field Division in San Antonio. And now we will proceed.

Ms. Lanius, welcome. You may proceed.

STATEMENT OF STACEY LANIUS, PLANO, TEXAS

Ms. LANIUS. Chairman Johnson, Members of the Subcommittee, thank you for inviting me to testify today about my personal experience with identity theft.

During 1986, I was a sophomore at the University of Texas at Austin. At that time, I was using my maiden name Stacey Rogers. An organization on campus was doing a fundraiser that involved credit card application. There were groups of five applications and the organization made money off of each group of cards that an individual applied for. The cards were MasterCard, Neiman Marcus, Sears, Zales Jewelry Store and Dillard's. I remember.

I asked my parents if I could apply for the cards to help my classmate with her fundraising project. My parents thought this was a good idea so that I could start building a credit history. Of course, they cautioned me about overusing the cards. I completed the five applications but never heard anything back. I was not worried. I assumed that because I was a full-time student with limited income the companies had denied my application.

Two years later, I made a purchase in Dillard's department store and paid by check. The clerk denied my check and told me I had to go to Customer Service. At Customer Service, I was told that I had exceeded my limit on my Dillard's credit card and was behind

on my payment. I told the clerk I didn't have a Dillard's credit card and asked to see the transactions on the account. There were numerous transactions on the account spanning two years.

I was able to obtain copies of the receipts for these purchases and on one single receipt the store clerk had asked for a driver's license so there was a driver's license number for me. My father was an FBI agent and I asked him to run the license and we discovered that a woman who shared my name, Stacey Rogers, was the one who made the purchases.

At the time, there was no Internet so I drove to the credit bureaus and requested copies of my credit report. This woman had somehow intercepted the five credit card applications for which I had applied two years before. She changed the address on the accounts so that when the cards were issued, they went straight to her. I never knew I had been approved for the cards. My best guess at the time that was that she worked at the business that processed the applications, saw that we shared the name and altered the applications. She also kept my Social Security number for future use.

On my credit reports, those five accounts were charged to the max and were all delinquent. Additionally, she had used my Social Security number to apply for more credit and financing. There were thousands of dollars in charges and numerous delinquent accounts on my credit history due to this theft of my identity.

In 1988 when I graduated and went to work for KPMG, my poor credit history followed me as it did for years; when I tried to get my first apartment lease, when I tried to purchase my first car, when I tried to actually apply for a credit card. And someone, the other Stacey Rogers, continued to use my Social Security number to finance everything from televisions to surgeries.

Each time I would go to a vendor to explain the problem or go to the credit bureaus to get the fraudulent purchases off my credit report, I was told that I needed to prove I had not made the purchases. How does one go about proving such a negative? I diligently visited every credit bureau, circling the accounts I claimed were fraudulent. The accounts stayed on my record, but a note was added there was a claim of fraud on the account.

In 1991, I married and my legal name changed. Several years later I finally noticed a decrease in fraudulent activity. I now have an excellent credit rating, have successfully financed the purchase of two homes and am free of the effects of the identity theft. However, the stress that that caused was tremendous occurring at a point in my life when I was just getting started as an adult. I now guard my Social Security number very carefully and try to check my credit on an annual basis.

Mr. Chairman, thank you again for this opportunity to share my story. I would be happy to answer any questions you or the other members may have.

Chairman JOHNSON. Thank you, ma'am. We appreciate you being here. We'll postpone the questions until everyone has testified.

[The prepared statement of Ms. Lanius follows:]

U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Social Security
Statement for the Record
Field Hearing on Social Security Numbers and Child Identity Theft
Stacey Lanius
September 1, 2011

Chairman Johnson and members of the subcommittee, thank you for inviting me to testify today about my personal experience with identity theft.

During 1986, I was a sophomore at the University of Texas at Austin. At that time I was using my maiden name: Stacey Rogers. An organization on campus was doing a fundraiser that involved credit card applications. There were groups of five applications and the organization made money off of each group of cards an individual applied for. The cards were: Mastercard, Neiman Marcus, Sears, Zales Jewelry Store and Dillards.

I asked my parents if I could apply for the cards to help my classmate with her fundraising project. My parents thought this was a good idea so that I could start building credit. Of course they cautioned me about overusing the cards.

I completed the five applications but never heard anything back. I was not worried. I assumed that because I was a full-time student with limited income the companies had denied my application.

Two years later, I made a purchase in Dillards and tried to pay by check. The clerk denied my check and told me that I had to go to Customer Service. At Customer Service I was told that I had exceeded my limit on my Dillards credit card and was behind on my payments. I told the clerk that I did not have a Dillards credit card and asked to see the transactions on this account. There were numerous transactions on the account spanning two years. I was able to obtain copies of the receipts for the purchases, and on one of the receipts was a driver's license number.

My father (an F.B.I. Agent) ran the license number for me and we discovered that a woman who shared my name, Stacey Rogers, had made the purchases. At the time, there was no internet, so I drove to the credit bureaus and requested a copy of my credit report. This woman had somehow intercepted the five credit card applications for which I had applied two years before. She changed the address on the accounts so that when the cards were issued they went straight to her. I never knew I had been approved for the cards. Our best guess at the time was that she worked at the business that processed the applications, saw that we shared a name, and altered the applications. She also kept my Social Security number for future use.

On my credit report those five accounts were charged to the max and were delinquent. Additionally, she had used my Social Security number to apply for more credit and financing. There were thousands of dollars in charges and numerous delinquent accounts on my credit history due to this theft of my identity.

In 1988 I graduated and went to work for KPMG. My poor credit history followed me for years, when I tried to get my first apartment lease, when I tried to purchase my first car, when I tried to actually apply for a credit card, and so on. The other Stacey Rogers continued to use my Social Security number to finance everything from televisions to surgeries. Each time I would go to a vendor to explain the problem, or go to the credit bureaus to get the fraudulent purchases off my credit report, I was told that I needed to prove that I had not made the purchases. How does one go about proving a negative?

I diligently visited every credit bureau, circling the accounts that I claimed were fraudulent. The accounts stayed on my record, but a note was added that there was a claim of fraud on the account. In 1991, I married and my legal name changed. Several years later, I finally noticed a decrease in the fraudulent activity.

I now have an excellent credit rating, have successfully financed the purchase of two homes and am free of the effects of the identity theft. However, the stress the theft caused was tremendous; occurring at a point in my life when I was just getting started as an adult. I now guard my Social Security number very carefully and try to check my credit on an annual basis.

Mr. Chairman, thank you again for this opportunity to share my story. I would be happy to answer any questions you or the other members may have.

Chairman JOHNSON. Mr. Bryson, you're recognized. Five minutes.

STATEMENT OF STEVE BRYSON, ALLEN, TEXAS

Mr. BRYSON. Thank you, Mr. Chairman. I would like to thank Congressman Johnson and the Members of the Subcommittee for allowing me to tell my family's story concerning identity theft.

A couple years ago my 17-year-old stepdaughter applied for a lifeguard job at a church camp in a summer job in Tyler, Texas. One of the prerequisites of this job was a simple background check of all employees by using Social Security numbers. This was done through the Safe Churches Project of Safe Advantages Services, which is a member of the First American family of companies.

My daughter submitted her Social Security number to the church and a background check was run. A few weeks later, we received a result of that check and were shocked to that find her Social Security number was being used by six to seven people in California, Nevada and Texas. In one case, two people living at the same address in Houston, Texas were using this number.

The Social Security number was assigned to her when she was born February 12, 1993; and since she was a minor, there was no reason for us to monitor or have any issue with it. Upon learning about this number of people, my wife contacted the local Social Security office here in Collin County and was informed that since she was a minor, there was very little they can help with.

I contacted a friend of mine in Tyler, Texas who's a retired FBI agent and he said that there was very little the Federal Government could or would do to help, and he said the only recourse we had was to contact the various credit agencies around the country and to send letters to the police and sheriff's departments in the cities where these individuals lived.

We contacted the credit rating agencies first and found that there was very little help due to the fact, again, that she was a minor. They did not even have her listed. At the time, we felt that there was no help and attempts to monitor or control. This was useless. It would cost a lot of money and a lot of time.

It's my opinion that her Social Security number was purchased, that these people purchase these numbers and that most probably they were here in the United States illegally. Identity theft is a crime whether you are buying, selling or using the Social Security number. This is a problem that seems to be growing daily. And I'm concerned that this is not being made a top priority by the Federal Government.

Chairman Johnson, I have no idea how this—what definitive impact this will have on my daughter now or in the future, but I do feel like at some point in time this will come up. In the mean time, there are at least six people who are out using her Social Security number who obtain jobs, credit, loans, possibly some type of benefits under Social Security.

Mr. Chairman, in conclusion, I do not believe that it should be the sole responsibility of the individual who is the victim of identity theft to attempt to correct these problems. I thank you again for your time and the Committee.

Chairman JOHNSON. Thank you, sir. I agree with you, we need to help you if we can. That's why we're having this hearing today.

[The prepared statement of Mr. Bryson follows:]

U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Social Security
Statement for the Record
Field Hearing on Social Security Numbers and Child Identity Theft
Steve Bryson
September 1, 2011

I would like to thank Congressman Johnson and the members of the Subcommittee for the invitation to tell my family's story concerning identity theft.

Two year ago when my step-daughter was 17 years old, she applied for a lifeguard job in Tyler, Texas with Green Acres Baptist Church summer camp at Lake Tyler. In order to obtain the job, the church required a simple background check on all employees by using Social Security numbers which were run through the "Safe Churches Project of Safe Advantage Services" a member of the First American Family of Companies. My daughter submitted her SSN to the church and they ran the background check.

When they sent us the results of that check we were shocked to find that her Social Security number was being used by six to seven other people in California, Nevada and Texas. In one case, two people living in Houston at the same address were using her number. This Social Security number was assigned to her when she was born on February 12, 1993 in Houston, TX and since she was a minor, the need to check her identity had never come up.

Upon learning of this, my wife contacted the local Social Security office in Collin County, Texas and was informed that there was very little they could do to help us. I contacted a friend in Tyler, Texas who had retired from the FBI a few years back and he told us that there was very little that the federal government could or would do to help and that the only recourse we had was to contact the various credit rating agencies in the U.S. and to send letters to local police and sheriff's office in the cities where these individuals lived. We contacted the credit rating agencies, but since she was under the age of 18, they didn't even have her listed and offered no help whatsoever. At this time we felt like there was no help and any attempts to monitor or control this was useless without spending a large amount of time and money.

It is my opinion that the people using her Social Security number purchased the number and identity from someone else and that perhaps some of these people are in the United States illegally. Identity theft is a crime and if you are selling or buying Social Security numbers, you are committing a crime. This is a problem that seems to be growing daily and I am concerned that government is not making fighting identity theft a top priority.

Chairman Johnson, I have no idea if this will have any definitive impact on my daughter but believe that one day it will be a problem. In the meantime, there are at least six other people who are illegally using her Social Security number to obtain jobs, credit, loans and possibly claiming some type of benefit under Social Security.

Mr. Chairman, in conclusion I do not believe that it should be the sole responsibility of the individual who is a victim of identity theft to attempt to correct these problems stemming from identity theft.

Thank you again for the opportunity to testify before this Subcommittee.

Chairman JOHNSON. Ms. Kueckelhan, welcome. You may proceed.

STATEMENT OF DEANYA KUECKELHAN, DIRECTOR, SOUTHWEST REGION, FEDERAL TRADE COMMISSION, DALLAS, TEXAS

Ms. KUECKELHAN. Thank you, sir. Chairman Johnson, Congressman Brady and Congressman Marchant. I'm Deanya Kueckelhan, Director of the Federal Trade Commission, Southwest Region, located here in Dallas and actually a native Texan. I have the privilege today of presenting the Federal Trade Commission's remarks on child ID theft.

It is so unfortunate to hear the two stories that were just told. We've just heard that our children do become victims of identity theft. Identity thieves steal, deliberately steal a child's ID. They fabricate a Social Security number coincidentally that sometimes belongs to a child and they do that to obtain employment, to receive government benefits or to obtain a loan for credit. The Federal Trade Commission's 2010 Consumer Signal Network Data Book shows that Texas ranks 5th among the states in ID theft complaints after Florida, Arizona, California and Georgia. And that's with over 24,000 complaints filed in the year of 2010 alone.

A non-FTC study shows that 142,000 instances of identity fraud are perpetrated on minors in the U.S. each year. So child identity theft is especially harmful, though, Chairman Johnson, because it can go on so long undetected, until a child becomes an adult and perhaps applies for a college loan or a car loan or seeks employment.

For this and other reasons, the Federal Trade Commission and DOJ's Office For Victims of Crime recently co-hosted Stolen Futures: A Forum On Child ID Theft on July 12th, 2011, this summer in Washington. We gathered panelists such as educators or child advocates and representatives of government agencies in the private sector as well as legal service providers and they discussed how to deter and remedy child ID theft.

Panelists noted, among many other things, that identity thieves steal a child's ID from schools, from businesses, from government agencies and, unfortunately, panelists also discussed the fact that sometimes friends and desperate family members will use the ID of a child in hard economic times when they have a lack of access to credit. They become desperate to use that child's social security

number in order to pay basic services such as heat or electricity or other utilities.

Panelists also talked about sensitive health information, particularly related to the foster care system. Panelists stated that in the foster care system a child's information is circulated through the Social Services network as well as in school records which makes foster children particularly vulnerable to child ID theft. In essence, a child's ID is a blank slate and because of the unique qualities of child ID theft, oftentimes makes it more valuable to steal a child's ID than an adult's ID.

Panelists also noted, as did Mr. Bryson, that the challenge this causes because parents don't routinely check a child's credit primarily is that children don't have a credit history; thus, parents have no reason to suspect a problem. One possible solution was mentioned by a panelist from the Utah Attorney General's Office, who described a proposed Utah initiative that would enable parents to enroll their child in a state identity protection program. Utah would pass the child's information on to TransUnion, which would in turn place a high risk alert on the child's name and information.

Panelists throughout the day stressed prevention. Controlling and limiting access to a child's information is one of the best ways to deter child ID theft. Panelists recommended that parents and guardians and foster care parents challenge routine request for their children's ID. Shall I go on?

Chairman JOHNSON. Continue.

Ms. KUECKELHAN. Thank you. Panelists also suggested that parents learn how their children are using the Internet and Social media because children sometimes innocently divulge their personal information that could be used to commit ID theft. Panelists also encouraged increased outreach to foster care workers and directly to the foster youth, especially the older teen foster youth who are about to enter the adult world and exit the foster care system.

The FTC's primary goal in co-hosting Stolen Futures was to learn more about this problem and develop messages for outreach. The FTC has already prepared new educational materials. I'm proud to say, they're already being distributed. We consulted with DOE on a back to school alert. We have it today on one of the tables upstairs. We will continue to distribute these. And I'm happy to answer questions.

Chairman JOHNSON. Thank you, ma'am.

Ms. KUECKELHAN. Thank you.

Chairman JOHNSON. You know, a lot has started when we started giving out numbers at birth. And, you know, I don't know how many babies get credit, but I doubt very many of them do, and so that's caused a lot of problems. We're looking at that aspect of it, too.

[The prepared statement of Ms. Kueckelhan follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON SOCIAL SECURITY

of the

HOUSE COMMITTEE ON WAYS AND MEANS

on

Child Identity Theft

Field Hearing
Plano, Texas

September 1, 2011

I. INTRODUCTION

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, I am Deanya Kueckelhan, Director of the Southwest Regional Office of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on child identity theft. Protecting consumers – especially vulnerable consumers such as children – against identity theft and its consequences is a critical component of the Commission's consumer protection mission.[2]

This testimony begins by describing the nature of identity theft generally and the Commission's law enforcement, nationwide complaint management, and education and outreach efforts on identity theft. In particular, it describes some of the 34 actions the Commission has brought since 2001 against businesses that allegedly failed to reasonably protect sensitive consumer information that they maintained. It then describes *Stolen Futures*, a recent forum on child identity theft held on July 12, 2011, co-sponsored by the FTC and the Department of Justice's Office for Victims of Crime. Finally, the testimony discusses next steps to combat this problem.

---

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

[2] *See* Identity Theft and Assumption Deterrence Act, Pub. L. 105-318, 112 Stat. 3007 (1998). Criminal prosecutions under the Act are handled by the United States Department of Justice. The Act directs the FTC, a civil law enforcement agency, to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education. The repository of identity theft complaints, known as the "Identity Theft Clearinghouse," is discussed in greater detail below in Section II.

II. IDENTITY THEFT

Millions of consumers are victimized by identity thieves each year,[3] collectively costing consumers and businesses billions of dollars[4] and countless hours to repair the damage. Given the serious and widespread harm caused by identity theft, the Commission has devoted significant resources toward combating the problem, acting aggressively on three main fronts: law enforcement, nationwide complaint management, and education.

A. Law Enforcement

The Commission enforces a variety of laws requiring entities, in certain circumstances, to have reasonable procedures in place to secure consumer information so that it does not fall into the hands of identity thieves or other unauthorized persons. For example, the Commission's Safeguards Rule under the Gramm-Leach-Bliley Act establishes data security requirements for financial institutions.[5] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose consumer reports have a permissible purpose for receiving that information,[6] and imposes safe disposal

---

[3] *See* Bureau of Justice Statistics, *National Crime Victimization Survey Supplement, Victims of Identity Theft, 2008* (Dec. 2010) ("BJS Supplement") at 1-2 (finding 11.7 million persons, representing 5% of all Americans age 16 or older, were victims of identity theft during a two-year period ending in 2008).

[4] *Id.* at 4 (finding the total financial cost of identity theft was 17.3 billion dollars during a two-year period ending in 2008).

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

[6] 15 U.S.C. § 1681c.

obligations on entities that maintain consumer report information.[7] In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices[8] in cases where a business makes false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury that is not reasonably avoidable by consumers and not outweighed by countervailing benefits.

Since 2001, the Commission has brought 34 law enforcement actions against businesses that allegedly failed to reasonably protect sensitive consumer information that they maintained. One of the best-known FTC data security cases is the 2006 action against ChoicePoint, Inc., a data broker that allegedly sold sensitive information (including Social Security numbers ("SSNs") in some instances) concerning more than 160,000 consumers to data thieves posing as ChoicePoint clients.[9] In many instances, the thieves used that information to steal the consumers' identities. The Commission alleged that ChoicePoint failed to use reasonable procedures to screen prospective purchasers of the consumers' information and ignored obvious security red flags. For example, the FTC alleged that the company approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from public commercial photocopying facilities. In settling the

---

[7] *Id.* at § 1681w. The FTC's implementing rule is at 16 CFR Part 682.

[8] 15 U.S.C. § 45(a).

[9] *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006).

case, ChoicePoint agreed to pay $10 million in civil penalties for violations of the FCRA and $5 million in consumer redress for identity theft victims, and agreed to undertake new data security measures.[10]

Most recently, in June of this year, the Commission resolved allegations that Ceridian Corporation[11] and Lookout Services, Inc.,[12] violated the FTC Act by failing to implement reasonable safeguards to protect the sensitive consumer information they maintained. The companies offered, respectively, payroll processing and immigration compliance services for small business employers. As a result, they both obtained, processed, and stored highly-sensitive information – including SSNs – of employees. The Commission alleged that both companies failed to appropriately safeguard this information, which resulted in intruders being able to access it. The orders require the companies to implement comprehensive data security programs and obtain independent audits for 20 years.

B. Nationwide Complaint Management and Analysis

In addition to law enforcement, the Commission collects, manages, and analyzes identity theft complaints in order to target its education efforts and assist criminal law enforcement authorities. The Commission manages the Identity Theft Clearinghouse, a secure online

---

[10] In 2009, the Commission charged that the company violated the earlier court order and obtained a stipulated modified order under which ChoicePoint agreed to expand its data security obligations and pay monetary relief in the amount of $275,000. *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Ga. 2009) (settlement entered on Oct. 14, 2009).

[11] *Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* www.ftc.gov/opa/2011/05/ceridianlookout.shtm.

[12] *Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* www.ftc.gov/opa/2011/05/ceridianlookout.shtm.

database of identity theft-related complaints. Identity theft victims can enter complaint information directly into the database via an online complaint form or by calling a toll-free identity theft hotline and speaking with a trained counselor. The Commission makes the Clearinghouse data available to over 2,000 American and Canadian federal, state, and local law enforcement agencies who have signed confidentiality and data security agreements.[13] Through the Clearinghouse, law enforcers can search identity theft complaints submitted by victims, law enforcement organizations, and the Identity Theft Assistance Center, a not-for-profit coalition of financial services companies. To assist law enforcement and policy makers, the FTC also routinely issues reports on the number and nature of identity theft complaints received by the FTC.[14]

C. Consumer, Business, and Other Education

Consumer education and outreach is another important part of the Commission's mission. The Commission works to empower consumers by providing them with the knowledge and tools to protect themselves from identity theft and to deal with the consequences when it does occur. The Commission receives on average 35,000 consumer contacts each week through its toll-free hotline and dedicated website, of which approximately 5,600 are identity theft

---

[13] For example, each of the 50 Offices of the Attorney General has access to the Clearinghouse data.

[14] *See, e.g.*, FTC, *Consumer Sentinel Network Data Book for January - December, 2010* (Feb. 2011), *available at* http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf. The 2010 Data Book shows that over 250,000 consumers reported some form of identity theft, which represents 19% of the total number of complaints submitted to the Commission. This makes identity theft the most frequently reported category of consumer complaints, continuing a pattern that started over a decade ago. The Data Book also shows that Texas ranks fifth among the states in identity theft complaints after Florida, Arizona, California, and Georgia, with 24,158 complaints submitted to the Commission (96.1 complaints per 100,000 population) during the time period measured.

complaints. Callers to the hotline receive counseling from trained personnel on steps they can take to prevent or recover from identity theft.

Further, the FTC makes available a wide variety of consumer educational materials, including many in Spanish, to help consumers deter, detect, and defend against identity theft. For example, the FTC publishes a victim recovery guide – *Take Charge: Fighting Back Against Identity Theft*[15] – that explains the immediate steps identity theft victims should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report;[16] and how to protect their personal information. The Commission has distributed over 3.8 million copies of the recovery guide and has recorded over 3.5 million visits to the Web version.

The Commission also sponsors a multimedia website, OnGuard Online,[17] designed to educate consumers about basic computer security, including the importance of not disclosing personal information such as SSNs to possible fraudulent operators. OnGuard Online was developed in partnership with other government agencies and technology companies. Visitors to

---

[15] *Available at* www.ftc.gov/bcp/ed/pubs/consumers/idtheft/idt04.pdf.

[16] The FCRA also provides identity theft victims with additional tools to recover from identity theft. For example, identity theft victims who provide police reports to a consumer reporting agency may obtain a seven-year fraud alert on their credit files, alerting potential users of their reports to exercise special vigilance in opening accounts in the consumers' names. In addition, victims may block fraudulent information on their credit files, obtain from creditors the underlying documentation associated with transactions that may have been fraudulent, and prohibit creditors from reporting fraudulent information to the consumer reporting agencies. *See* FCRA, 15 U.S.C. §§ 605A, 605B, 609(e), and 611.

[17] *Available at* www.OnGuardOnline.gov. A Spanish-language counterpart, Alerta En Linea, is available at www.AlertaenLinea.gov.

the site can download educational games and videos, learn more about specific topics, including phishing and social networking, and obtain useful tips and information in an interactive format.

The Commission directs its outreach to businesses as well.[18] It has developed a brochure and an online tutorial[19] that set out the key components of a sound data security plan. These materials alert businesses to the importance of data security and give them a solid foundation on how to address those issues. In addition, the FTC creates business educational materials to address particular risks. For example, the Commission developed a new business education brochure – *Peer-to-Peer File Sharing: A Guide for Business*[20] – to educate businesses about the risks associated with P2P file sharing programs and advise them about ways to address these risks.

Further, the Commission leverages its resources by providing educational and training materials to "first responders." For example, because victims often report identity theft to state and local law enforcement agencies, the FTC offers resources to law enforcers on how to talk to victims about identity theft.[21] The Commission also distributes a law enforcement resource CD Rom that includes information about how to assist victims, how to partner with other law enforcement agencies, how to work with businesses, and how to access the Identity Theft

---

[18] *See* FTC, *Protecting Personal Information: A Guide for Business;* and FTC, *Information Compromise and Risk of Identity Theft: Guidance for Your Business.* Both publications are available at http://business.ftc.gov.

[19] The tutorial is available at www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html.

[20] *Available at* www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm. Peer-to-Peer (P2P) technology enables companies to form a network in order to share documents and to facilitate online telephone conversations.

[21] Resources for law enforcement are available at www.ftc.gov/idtheft.

Clearinghouse. In addition, the FTC and its partners have provided identity theft training to over 5,400 state and local law enforcement officers from over 1,770 agencies.

Finally, the FTC has encouraged the development of a nationwide network of *pro bono* clinics to assist low-income identity theft victims. As part of this initiative, the FTC has created a comprehensive guide for advocates providing legal assistance to identity theft victims. The Guide for Assisting Identity Theft Victims (*Pro Bono Guide*)[22] describes how advocates can intervene with creditors, credit reporting agencies, debt collectors, and others, and it provides self-help measures that victims can take to address their problems. Step-by-step instructions provide best practices for recovering from identity theft.

III. CHILD IDENTITY THEFT

In addition to its general efforts to combat identity theft, the Commission often examines how to target its outreach efforts toward vulnerable populations, such as children who have been victims of identity theft. Through a variety of means, identity thieves may deliberately capture and use a child's SSN, or fabricate a SSN that coincidentally has been assigned to a child, in order to obtain employment, apply for government benefits, open new accounts, or apply for car loans or even mortgages. Indeed, one study has estimated that 142,000 instances of identity fraud are perpetrated on minors in the United States each year.[23] Another study of 40,000

---

[22] The *Pro Bono Guide* is available at www.idtheft.gov/probono.

[23] *See* ID Analytics, *More Than 140,000 Children Could Be Victims Of Identity Fraud Each Year* (July 12, 2011), *available at* www.idanalytics.com/news-and-events/news-releases/2011/7-12-2011.php. ID Analytics noted, however, that this figure is under-representative of the actual rate of child identity theft because the sample was self-selected, focusing on children enrolled in their service, and likely does not include instances of parents who may victimize their own children, nor does it reach all uses of child data for fraud (e.g., medical claims, government benefits, employment).

children who had been enrolled in an identity protection service found that 4,311 of those children – or 10.2% – had loans, property, utility, and other accounts associated with their SSNs.[24] Child identity theft is especially pernicious because the theft may not be detected until the child becomes an adult and seeks employment, or applies for student and car loans.

To help address the challenges raised by child identity theft, Commission staff, along with the Department of Justice's Office for Victims of Crime, recently hosted *Stolen Futures: A Forum on Child Identity Theft*.[25] Panelists, including educators, child advocates, legal services providers, and representatives of various governmental agencies and the private sector, discussed how to prevent and remedy child identity theft. Below is an overview of the discussions that took place at the forum and recommendations for next steps.

A. The Child Identity Theft Forum Discussions

First, panelists focused on the causes of child identity theft. They noted that identity thieves often steal children's information from schools, businesses, and government agencies. Panelists also noted that friends and family members may use children's identities, particularly when they fall on hard economic times.[26] Indeed, a lack of access to credit may cause family members – including extended family members – to use the identities of children in their

---

[24] *See* Richard Powers, Carnegie Mellon CyLab, *Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers* (2011), *available at* www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf.

[25] *See* www.ftc.gov/bcp/workshops/stolenfutures (also containing a link to a webcast and transcripts of the Forum); *see also* Press Release, *FTC, Department of Justice to Host Forum on Child Identity Theft* (June 2, 2011), *available at* www.ftc.gov/opa/2011/06/childtheft.shtm.

[26] *See generally* Transcript of Stolen Futures, Session 2, Remarks of Linda Foley, Russell Butler, and Theresa Ronnebaum, *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#July12_.

households in order to pay basic expenses, such as heat and other utilities. In addition, several panelists noted that sensitive health and other personal information of children in foster care is often circulated widely within the schools and social services networks, leaving foster children particularly vulnerable to identity theft.[27]

Second, panelists discussed the unique challenges created by child identity theft. For example, a child's unused SSN is uniquely valuable to a thief because it typically lacks a previous credit history and can be paired with any name and birth date. In effect, a child's identity is a blank slate that can be used to obtain goods and services over a long time period because parents typically do not monitor their children's credit, often having no reason to suspect any problem.

In addition, while businesses can often detect instances of fraud involving adults by comparing an adult's SSN against a fraud or other commercial database, the same does not hold true for children, who typically lack an established credit history. Indeed, fraud alerts, a key tool used by adult victims of identity theft to warn potential creditors of possible identity theft, are premised on the existence of a credit file. Parents ordinarily cannot place a fraud alert on their child's credit file if the child has no such file.

Further, remedies available under federal law – such as extended fraud alerts, access to documents underlying the theft, and blocking of erroneous debts – typically require a victim to obtain a police report to document the crime. Panelists noted that children victimized by parents

---

[27] *See* Transcript of Stolen Futures, Session 1, Remarks of Matt Cullina, *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#July12_.

or guardians are often reluctant to file a police report naming a loved one or a source of financial support as the perpetrator.[28]

Third, panelists discussed potential solutions to the problem. A representative from the Utah Attorney General's Office discussed a Utah initiative that would enable parents to enroll their child in a state identity protection program. Utah would pass the child's information onto TransUnion, which would in turn place a "high risk" alert on the child's name and SSN.[29] This program would help prevent an identity thief from attempting to obtain credit in the child's name or SSN. According to the Utah representative, Utah would like to work with other states to expand the program nationwide, once it is fully implemented.[30]

Private solutions were also discussed. Parents may enroll their children in a monitoring service to detect possible early signs of identity theft. One approach scans children's personal information to determine whether there are matches in various credit and other databases. Another approach provides alerts to parents if a child's personal information is being used in credit and other commercial transactions, such as a new credit application. Both of these approaches require additional investigation to confirm actual child identity theft because the use

---

[28] *See generally* Transcript of Stolen Futures, Session 2, Remarks of Linda Foley, Russell Butler, and Theresa Ronnebaum, *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#July12_.

[29] *See generally* Transcript of Stolen Futures, Session 4, Remarks of Richard Hamp, *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#July12_.

[30] Mr. Hamp also explained that Utah has considered expanding the program to enable TransUnion to suppress erroneous information already existing in a child's file. However, the necessary steps to authenticate the child's identity appear to be cost-prohibitive at this time.

of a child's SSN could be an innocent mistake, such as the result of a transposed number. Panelists encouraged further study of these types of solutions.

Finally, panelists discussed the importance of prevention. Controlling and limiting access to a child's information is one of the best ways to protect children from identity theft, and panelists suggested several ways to do so. For example, panelists recommended that parents and guardians challenge requests for their child's SSN and other personal information. They should ask why information is being collected and how it is going to be used. Panelists also suggested that parents and guardians learn how their child uses the internet and social media, so that children do not divulge personal information that could be used to commit identity theft. As to child identity theft in the foster care system, panelists encouraged increased outreach to over-burdened case-workers, who may be unaware of the problem and do not know how to protect against it. They also encouraged increased outreach directly to foster youth, especially older teens who are soon to exit the foster care system. For example, one pilot program in California, the First Star UCLA Bruin Guardian Scholars Summer Academy, provides a free five-week curriculum that teaches foster youth various skills, including how to be their own advocates regarding their credit and personal information.[31] The organizers of this program, which currently serves thirty youths, hope to replicate it nationally.

B. Next Steps

The Commission's primary goal in co-hosting the forum was to learn more about the problem of child identity theft and to develop messages and target audiences for outreach on this issue. Based on the discussions from the forum, the Commission staff is preparing new

---

[31] *See* www.guardianscholars.ucla.edu/docs/Application%20Packet%202011.pdf.

educational materials in several areas. First, the staff is developing a "back-to-school alert," educating parents on the importance of safeguarding children's information in schools. The Commission staff has worked collaboratively with the Department of Education on this alert. Second, staff is working on new education materials for parents – to be distributed widely through local and community organizations – on how to prevent child identity theft, how to protect children's personal data, and how to help their children who have been victims of identity theft. Third, staff plans to conduct outreach to foster care advocates to find ways to better assist foster care youth both in protecting their personal data and in removing bad debts fraudulently incurred in their name. Fourth, staff plans to conduct outreach to social workers, legal services officials, and others who believe a child has been the victim of familial identity theft. Finally, staff plans to develop outreach materials specifically designed for young adults who learn that they have been identity theft victims. Commission staff remains open to additional approaches and will work with other federal and state agencies, private industry, and non-profit legal service providers and other organizations to develop outreach programs to combat child identity theft. Of course, in addition to targeting its outreach efforts, the agency will continue its robust efforts to address all forms of identity theft – through law enforcement, partnerships with state and federal agencies, nationwide data management and analysis, and education.

IV. CONCLUSION

The Commission will continue to play a central role in the battle against identity theft, including child identity theft, and looks forward to working with you on this important issue.

Chairman JOHNSON. Dr. Vieraitis, welcome. Please go ahead.

STATEMENT OF LYNNE M. VIERAITIS, PH.D., ASSOCIATE PROFESSOR OF CRIMINOLOGY, UNIVERSITY OF TEXAS AT DALLAS, RICHARDSON, TEXAS

Dr. VIERAITIS. Thank you. Chairman Johnson, Members of the Committee, thank you for inviting me to discuss my research on identify theft at this hearing today. By presenting the perspectives of offenders, I hope to provide the Committee with a more comprehensive picture of identity theft, one that may offer suggestions of how it might be better controlled.

The 9/11 highjackers, a single mother in Texas addicted to methamphetamine, a married father of three and college graduate, the girlfriend of a gang member of one of the most notorious Latin American gangs operating in the United States, they appear to share little in common. The one thing they do share is they were all identity thieves.

I'm often asked to describe the typical identity thief; but as the aforementioned profiles suggest, it is difficult to paint a portrait of a typical one. The identity thieves we spoke with came from all walks of life and had diverse criminal histories. Their backgrounds ranged from upper to lower class, the unemployed to employed, from day laborers to professionals, middle school drop-outs to college graduates and from those with lengthy criminal histories to first-timers.

We found that some thieves worked alone while others were involved in teams of up to 30 members. Some were fueled by their addictions to illegal drugs while others simply wanted to live above their means or meet day-to-day living expenses. The diversity in their backgrounds and current lifestyles influenced the ways in which they chose to carry out their crimes.

So how do they steal information and what do they do with it? Those who worked alone typically used personal information of others to open credit card accounts or secure bank loans. In some cases, they used information available to them from their place of work. In some cases they used the information of family members, including their own children and friends. Other thieves used more sophisticated and elaborate schemes to dupe strangers into revealing their information. For example, one set up a fake employment site with applicants willingly supplying their information.

The majority of the identity thieves we interviewed operated in teams. Street level identity theft rings, or SLIT rings for short, relied on numerous methods to steal and convert information. Some rings paid employees of companies to get information on clients or customers. Others targeted residential and commercial mailboxes, but most SLIT rings bought their information from another street-level criminal who was typically engaged in drug sales, robbery, burglary or other street crimes who sold the information to the ring leader. This information included driver's licenses and Social Security cards stolen from homes or cars. Some ring leaders claim that acquaintances, friends and family members provided their information in exchange for a fee.

After stealing a victim's information, offenders applied for credit cards in the victim's names, opened new bank accounts, deposited counterfeit checks, withdrew money from existing bank accounts, applied for loans and opened utility or telephone accounts.

Such transactions also require some form of official identification. To produce these documents, teams recruited employees of state or federal agencies with access to Social Security cards or birth certificates which were then used to order identification cards. They were also able to manufacture false cards using rogue employees of state departments of motor vehicles or other street hustlers who had managed to obtain the necessary equipment.

Members of occupational teams use their legitimate place of employment to steal information and convert it to cash or goods acting almost exclusively with fellow employees to commit their crimes.

In addition to the question of how they do it, I'm often asked why they do it. The simple answer: It's quick and easy money. But the answer is more complex.

What we found when we spoke to offenders was that they engage in identity theft because they see it not just as financially rewarding but emotionally rewarding as well. They believe it to be relatively low in risk and find it easy to justify or excuse their actions. In short, they perceive the rewards to be high and the risks low.

The identity thieves we spoke with were confident in their ability to profit from their crimes and to avoid detection; despite the fact we were speaking to them while they were incarcerated. Most didn't focus on the risks of crime, but all actively engaged in strategies to reduce the likelihood of detection by victims, law enforcement and financial institutions, including reducing the number and amount of transactions they conducted per identity. They selected certain times, persons and places to cash in and tried to blend in as much as possible.

The crime of identity theft includes the acquisition of information as well as the use of that information. But there are several points along that crime continuum that can be addressed with policy. The challenge for policy makers and law enforcement is identifying policies and strategies that can target these weak points while at the same time allowing business and customers to conduct transactions.

Several suggestions for prevention are provided that draw upon several well known situational crime prevention techniques. Each of these strategies is more effective when they can be catered to highly specific forms of identity theft, for example, child identity theft versus adult and identity theft committed by loaners versus those committed by SLIT rings.

We must increase the effort and risk of obtaining information. We need to continue to promote awareness of identity theft and educate citizens on how to protect that information, and we may need specific guidance for parents to protect their children. We need to educate consumers on what to do when their identity is stolen and when it's used and encourage them to report to law enforcement. The National Crime Victimization Survey indicates that only 17 percent of the victims in their study reported it to law enforcement. We need to reduce unsafe business practices. Institutions that have data on children, including hospitals and schools should be particularly vigilant and we need to provide alternatives to agencies dealing with special populations, such as children in the foster care system.

We need to increase the effort and risk of converting information. Systems should be in place to verify and alert credit granting agencies and employers who verify employment eligibility that a Social Security number is issued to a person under the age of 18.

Chairman JOHNSON. Can you summarize?

Dr. VIERAITIS. I'm sorry?

Chairman JOHNSON. Can you summarize? Your time has expired. Can you summarize?

Dr. VIERAITIS. Yes. Increase the risk of getting caught. Very briefly, what we need to know, identity theft and perhaps child identity theft in particular poses a challenge for law enforcement. We need to know more about identity theft and those who commit it and be better and more consistent in measures of identity theft and fraud, specifically frauds that target children.

We need more systematic data collection from agencies responsible for personal information, agencies that use it, law enforcement agencies and from victims and from those who know most about how and why identity theft occurs, the identity thieves themselves. Thank you.

Chairman JOHNSON. Thank you.

[The prepared statement of Dr. Vieraitis follows:]

Testimony for the
House Committee on Ways and Means
Subcommittee on Social Security
Field Hearing on
Social Security Numbers and Child Identity Theft

Lynne M. Vieraitis, Ph.D.
Associate Professor of Criminology
University of Texas at Dallas

Qualifications

I have a PhD in criminology from Florida State University and am an associate professor of criminology at the University of Texas at Dallas. My research focuses on identity theft, specifically on those who choose to commit it, and has been supported by the National Institute of Justice.[1] I have published frequently in peer-reviewed journals, presented research findings for government agencies, including the Federal Trade Commission and the National Institute of Justice, as well as for various professional conferences and news media outlets. My co-author (Heith Copes) and I have a book, *Identity Thieves: Motives and Methods*, forthcoming from Northeastern University Press in spring 2012.

Summary

According to the most recent estimates from the National Crime Victimization Survey (NCVS), approximately 12 million persons or 5 percent of all persons age 16 or older were victims of at least one type of identity theft during 2006-2007.[2] These estimates are slightly higher than other estimates including those from the Federal Trade Commission (FTC), which estimates 8 million victims over the age of 18 years.[3] Unfortunately, as with most frauds, it is difficult to ascertain the true picture of the pervasiveness and costs of identity theft with the available data. One reason for the differences in estimates is that not all agencies define identity theft in the same way. For example, the NCVS considers credit card fraud in its estimates of identity theft, but other agencies do not. Since there is no universally accepted definition of identity theft we find differences not only on the estimates of the prevalence and costs of identity theft but also on the portraits of both victims and offenders. Another reason for the differences in estimates is that identity theft is likely an underreported type of crime. Moreover, underreporting by victims may be associated with the type of theft that occurs. Victims whose information is stolen and used by someone they know are less likely to report than those victimized by strangers. Some victims, as in the case of child identity theft, may not know they

---

[1] National Institute of Justice, Office of Justice Programs, U.S. Department of Justice (Grant No. 2005-IJ-CX-0012).
[2] Bureau of Justice Statistics. 2010. *Identity Theft Reported by Households, 2007—Statistical Tables.* Washington, DC: U.S. Government Printing Office
[3] Federal Trade Commission. 2009. *Consumer Sentinel Network Data Book for January to December 2008.*

have been victimized. Other differences may be attributed to the population from which the agency or company is sampling with some agencies relying on reports from victims, other agencies relying on local law enforcement data, and others on data from their own customers.

The problem with estimating prevalence of identity theft is exacerbated when the victims are children. Child victim identity theft can go unnoticed for many years; if not decades. It is often not until the victim begins to apply for credit that the theft or fraud is discovered. Additionally, if the child's information is being used by a parent, step-parent, sibling, or other family member, the likelihood that it is reported is much lower than if the child's information is being used by a stranger. Thus, the extent of child identity theft and whether it is growing is difficult to assess with existing data. The FTC has recently reported an increase in the number of child identity theft cases reported to their agency, but caution must be used when interpreting these results. It is possible that people are simply more likely to report identity theft than in previous years, are more aware of it, or shifts in the population age 18 years and older and the numbers applying for credit, including student loans may have changed. According to existing research, child identity theft makes up approximately 3 to 8 percent of all identity theft cases.[4]

What we do know is that there are millions of victims every year, there are billions of dollars lost (estimates range from $16 billion to $50 billion per year), and we know that US citizens are very concerned about identity theft and fraud.[5] Information is available from both public and private agencies that collect data on identity theft and suggest that identity theft is becoming more common and more costly. Yet, while much has been written about victims, prevention techniques, and state and federal legislation, little research has devoted attention to studying those who engage in identity theft.[6] Our research begins to fill this gap. By examining the perspectives of offenders, our goal was to produce a more comprehensive picture of identity theft, one that would offer suggestions for how identity theft might be better controlled.

The research I conducted with my colleague, Dr. Copes from the University of Alabama at Birmingham, is based on in-depth, face-to-face interviews with fifty-nine identity thieves.[7] The interviews were conducted with men and women serving time in federal prisons across the United States for violating the federal statute for identity theft (18 U.S.C. § 1028).

---

[4] Kresse, William, Kathleen Watland, and John Lucki. 2007. *Identity Theft: Findings and Public Policy Recommendations.* Final report to the Institute for Fraud Prevention http://www.sxu.edu/Academic/Graham/Documents/identitytheft_study.pdf).;Pontell, Henry N., Gregory C. Brown, and Anastasia Tosouni. 2008. Stolen Identities: A Victim Survey. In Crime Prevention Studies: Identity Theft and Opportunity, edited by Graeme Newman and Megan McNally. New York: Criminal Justice Press.

[5] Unisys. 2009. *Unisys Security Index Reveals High Concern among Americans about Government and Business Protection of Private Data.* Retrieved on January 20, 2010 (http://www.unisys.com).

[6] Most of what we know about identity thieves comes from closed case reports, either from the U.S. Secret Service or local police departments (e.g., Kresse et al; Allison, et al.). Allison, Stuart, Amie Schuck, and Kim M. Lersch. 2005. "Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/Offender Characteristics." *Journal of Criminal Justice* 33:19–29.

[7] We interviewed 65 individuals but six offenders claimed to be innocent of all charges by either denying they had taken part in or had knowledge of the identity theft (if they had co-defendants). Our findings are based on interviews with 59 identity thieves.

The motivation for our research was based on our belief that it is important to gain the offender's perspective when trying to improve our understanding of crime and to design policies aimed at curtailing it. Although gathering accurate information from victims, law enforcement officers and prosecutors is essential to understanding identity theft, we recognize that information from the identity thieves themselves also provides an important piece to the puzzle. With that goal in mind, we questioned identity thieves about their lives and crimes. We wanted to know: who engages in identity theft? Why do they choose identity theft instead of other types of crime? How do they organize themselves to commit their crimes? How do they acquire a victim's personal identifying information? What do they do with the information? What risks they associate with their crimes? What steps they take to avoid detection and capture? How their crimes eventually come to an end? By asking identity thieves to answer these questions in their own words, we hoped to better understand their motives for choosing identity theft, the methods they use to commit it, and the meaning all of this has for developing informed theory and policy.[8]

What We Learned

Who? Although I am often asked to describe the "typical" identity thief, it is difficult to paint a portrait of a "typical" one. Those we spoke with came from all walks of life and had diverse criminal histories. Their backgrounds ranged from the upper to lower class, the unemployed to the employed, from day laborers to professionals, middle-school dropouts to college graduates, and from those with lengthy criminal histories to "first timers." They ranged in age from 23 to 60 with a mean age of 38.

We found that some thieves worked alone, while others were involved in teams of up to 30 members. Some were fueled by their addictions to illegal drugs, while others simply wanted to live above their means. The diversity in their backgrounds and current lifestyles influenced the ways in which they chose to carry out their crimes. Our interviews revealed that identity thieves relied on three primary organization schemes to carry out their crimes: loners, street-level identity theft (SLIT) rings,[9] and occupational teams.

How? Twenty-four percent of the offenders in our sample were typed as loners. They typically used the personal information of others to open credit card accounts or secure bank loans. Many of these offenders claimed that they tried to make payments on the accounts to prevent victims from discovering the fraud, but eventually repayment became impossible. In some cases, they used information available to them for their place of work and in some cases they used the information of family members, including their own children, or friends. In one case, a woman employed at a mortgage company used client information to obtain personal bank

---

[8] Copes, Heith and Lynne M. Vieraitis. *Identity Thieves: Motives and Methods.* Boston: Northeastern University Press. (In Press).

[9] Pavlicek, Bruno. 2005. "Identity Theft and slit Rings: An Unrecognized yet Growing Cancer." *Crime and Justice International* 21:29–33.

loans. In another, the offender used the personal information of deceased family members to open bank accounts, get credit cards, and apply for a HUD loan. One thief used the personal information of her children and mother to take out bank loans. Other thieves used more sophisticated and elaborate schemes to dupe strangers into revealing their information. For example, one set up fake employment sites with applicants willingly supplying all their personal information, another used obituaries to access information and file fraudulent Medicare claims.

The majority of the identity thieves we interviewed operated in teams characterized by an elaborate division of labor in which members perform different roles depending on their knowledge and skills. There was considerable diversity among this group and necessitated the division of teams into two types: street level identity theft rings and occupational teams. SLIT rings and occupational teams share many similarities but they differ noticeably in the methods they use to steal and convert information.

SLIT rings relied on numerous methods to acquire and convert information. Some rings relied on an individual employed by a company that possessed legitimate access to names and personally identifying information of company or agency clients to get information. Others targeted residential and commercial mailboxes to steal checkbooks, bank statements, or medical bills. For most SLIT rings in our sample, the person supplying the information was a street-level criminal—typically engaged in drug sales, robbery, burglary, or other street crimes—who sold the information to the ringleader. This information included drivers' licenses and social security cards. Some rings obtained information from willing acquaintances, friends and family members in exchange for a fee. The "victim" would then wait a while before reporting the "theft." In one case involving a well-known gang, the ringleader paid someone to purchase birth certificates from drug addicted mothers. The birth certificates of US children were used to gain passports so the children of gang members and their associates could enter the country "legally."

After obtaining a victim's information, offenders applied for credit cards in the victims' names, opened new bank accounts and deposited counterfeit checks, withdrew money from existing bank accounts, applied for loans, or opened utility or telephone accounts. Because such transactions all require some form of official identification, the false identity document source played an important role. To produce these documents, teams recruited employees of state or federal agencies with access to social security cards or birth certificates, which could then be used to order identification cards. While thieves could use fraudulent information to obtain identification cards through conventional channels, it also was possible to manufacture false cards using rogue employees of state departments of motor vehicles, or through street hustlers who had managed to obtain the necessary equipment. (Some offenders specialize in the production of false identification cards for use by underage students to purchase alcohol and by illegal immigrants to apply for jobs.) For slit rings, the most common strategy for converting information into cash was by applying for credit cards, both from major card issuers and individual retailers. Offenders could use a stolen identity to order new credit cards, or to issue a duplicate card on an existing account. With these cards in hand, they could buy merchandise for their own personal use, for resale to friends and acquaintances, or to return for cash.

Another common strategy for converting information into cash or goods involved producing counterfeit checks. Offenders typically used such checks to open new bank accounts, or deposited them in the victim's existing account before withdrawing cash. Counterfeit checks also could be cashed at grocery stores, or used to purchase merchandise and pay bills.

Members of occupational teams used their legitimate place of employment to steal information and convert it to goods or cash, acting almost exclusively with fellow employees to commit their crimes. In mortgage fraud schemes, the majority of players were employed at the same company or at companies that worked together to process home loans. In cases involving workers at a state department of motor vehicles, an outside source provided information to employees, who then issued state identification cards or driver's licenses that were subsequently used to carry out identity thefts. The thefts committed by occupational teams typically involved theft on a larger scale, characterized by numerous victims and high dollar losses than those committed by SLIT rings or loners.

Why? In addition to the question, "how do they do it?" I am often asked "why they do it?" The simple answer is quick and easy money. Data from victims and law enforcement suggests that identity thieves are motivated by a desire for money, to avoid authorities, or to avoid using their own information to set up utility or cell phone accounts. These are all true, but merely skim the surface of offenders' motivations. It does not, for example, tell us why they choose identity theft instead of legitimate work or even other types of crimes. What we found was that offenders engage in identity theft because they see it as financially and emotionally rewarding, believe it to be relatively low in risk, and find it is easy to justify or excuse their actions. In short, they perceive the rewards to be "high" and the risks "low."

Consistent with research on persistent offenders, the identity thieves we spoke with were confident in their abilities to profit from their crimes and to avoid detection. Most didn't focus on the risks of crime, but all actively engaged in strategies to reduce the likelihood of detection. They spoke about the many ways in which they minimize the risk of detection by victims, financial institutions, and law enforcement. Briefly, they reduced the number and amount of transactions conducted with each identity, selected the right times, places and people to get and use information, and took steps to "blend in."

Policy Recommendations

The crime of identity theft includes the acquisition of information as well as the use of that information for ill gotten gains including avoiding bill collectors, law enforcement, opening bank accounts, taking out home, car and personal loans, etc. Thus, there are several points along the crime continuum that can be addressed through policy. The challenge for policymakers and law enforcement is identifying policies and strategies that can target these weak points while at the same time allowing businesses and customers to conduct transactions.

Several suggestions for prevention are provided that draw upon several well-known situational crime-prevention techniques, including increasing the effort the offender must use to acquire and convert information, increasing the risks of getting caught, and removing excuses that offenders may use to justify their crime. Each of these strategies is more effective when they can be catered to highly specific forms of identity theft (e.g., child identity theft vs. adult identity theft and identity theft committed by loners vs. those committed by SLIT rings).

- *Increase the Effort and Risk of Obtaining Information*
    - Educate consumers on ways to protect their identity. State and federal policymakers have made tremendous strides in passing legislation that attempts to reduce the opportunities for would-be identity thieves to steal information. We need to continue to promote awareness of identity theft especially to citizens who don't necessarily have easy access to information.
    - Educate consumers on what to do when their identity is stolen and when it is used.
    - Encourage individuals to report their victimization to law enforcement, federal agencies, and businesses. Require businesses to report theft of data in a timely manner.
    - Reduce unsafe business practices. It is essential that businesses and agencies whose employees are responsible for the handling of such information be trained properly on the best practices for protecting information and management should establish a set protocol for checking to ensure that employees are following these practices. Institutions that house data on children, including hospitals and schools, should be vigilant. Special populations, such as children in the foster care system should be issued an identification number when placed in a home. The social security number should only be used by the state agency to verify eligibility and issue benefits.
    - To the extent law enforcement and other agencies can reduce the number of individuals involved in other street crimes including, drug use, sales, and manufacturing, burglary, robbery, prostitution, etc. there will be fewer sources of information from which identity thieves can buy information.

- *Increase the effort and risk of converting information*
    - Educate and encourage victims to report their victimization immediately to all appropriate agencies. If someone is victimize by burglary, take steps with credit agencies just in case the offender has your information.
    - Reduce unsafe business practices and develop strategies to ensure employees are following the rules. Offenders say the scariest and riskiest part of identity theft is going to the bank or store to commit fraud. They know which stores check identification and under what conditions. It is important that all stores, banks, and other financial institutions follow policies carefully and consistently.
    - Systems should be in place to verify and alert credit granting agencies, for example, that a social security number is issued to a person under the age of 18 years.

- *Increase the risks of getting caught*
  - Encourage local law enforcement to devote time and energy to investigating identity theft.
  - Encourage investigators to consider that identity theft may be part of other street crimes such as residential burglaries, theft from motor vehicles, shoplifting, etc.
  - Develop strategies based on behavioral cues that businesses can incorporate into training employees. In most cases, the identity thieves regardless of how they acquired information were easily able to convert the information into cash or goods.
  - Consider expanding the definition of child abuse and neglect to include financial abuse and fraud.

What Remains to be Learned

We need better and consistent measures of identity theft and fraud, specifically those frauds that target children. We need more systematic data collection from agencies responsible for personal information, agencies that use personal information in legitimate business practices, from law enforcement agencies at local, state, and federal levels, from victims, and from those who know most about how and why identity theft occurs—the identity thieves themselves. From offenders, we need to know how they adapt to changes in technology and business practices, how they have responded to changes in legislation designed to prevent them from accessing information and converting that information into cash or goods and whether they target children and if so, why they do so. Child identity theft is harder to detect, harder for victims to report if they are victimized by someone they know, and harder to address particularly with our lack of data. It may occur over a longer period of time than other forms of identity theft making it not only more difficult to discover but more difficult for the victim to restore their "good name." It is important when developing policy that we clearly identify and understand the problem we are dealing with. Child identity theft that is facilitated by family members poses a different challenge for policymakers and law enforcement than does theft by organized criminal groups.

Chairman JOHNSON. Mr. Feldt, I understand you and Mr. Puente are going to share the time.

Mr. FELDT. Yes, sir.

Chairman JOHNSON. Thank you. You may proceed. Thank you.

STATEMENT OF ROBERT FELDT, SPECIAL AGENT-IN-CHARGE, OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, DALLAS FIELD DIVISION, DALLAS, TEXAS, ACCOMPANIED BY ANTONIO PUENTE SPECIAL AGENT, DALLAS FIELD DIVISION, SAN ANTONIO, TEXAS

Mr. FELDT. Good afternoon, Chairman Johnson, Members of the Subcommittee. My name is Robert Feldt. I'm the Special Agent In-Charge for Social Security OIG's Dallas Field Division, which handles Social Security fraud investigations in Texas and four other states. Thank you for the invitation to testify today.

According to identity theft experts, identity thieves target child Social Security numbers because a child's SSN is usually issued at

birth and not used for credit purposes for about 18 years. This allows for the potential long-term undetected abuse of a legitimate SSN, and the potential long-term harm to a young person's financial future.

We in the OIG appreciate the concern your Subcommittee has for families and their children with regard to identity theft, and we pursue as many SSN misuse cases as our resources allow. We receive thousands of SSN misuse allegations each year. Our agents participate in SSN issues task forces across the country investigating identity theft, as well as mortgage, bankruptcy and benefit fraud.

In fiscal year 2010, we had more than 400 SSN misuse cases that resulted in criminal conviction. Some of our most fulfilling cases are those that lead to the arrest of an individual who used someone else's SSN to collect Social Security benefits, because we're able to repair a person's identity and recover stolen agency funds.

Our agents have also recently reported a relatively new SSN issue scheme involving credit privacy numbers, or CPNs. These nine-digit numbers are sold by dishonest organizations usually on the Internet, to individuals with poor finances, with the promise the numbers will allow the individuals to create a new credit file. But consumers should know CPNs are not legal identification numbers. In fact, they are usually stolen SSNs, particularly those belonging to children, for the reasons I've mentioned.

Our investigative and audit work has taught us that the more SSNs are used in day-to-day transactions, the higher the probability these numbers can be stolen and used to commit crimes. We've made many recommendations to SSA related to SSN integrity, and we support this Subcommittee's efforts to limit the use and display of the SSN. That information is detailed in my written statement for the record.

In conclusion, OIG's investigators are committed to pursuing SSN misuse and identity theft cases. Our auditors and attorneys will also continue to make recommendations to your Subcommittee and to SSA to improve the integrity of SSNs, especially those belonging to children.

Thank you again for the invitation to testify. I will yield my remaining time to Special Agent Antonio Puente.

[The prepared statement of Mr. Feldt follows:]

U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Field Hearing on Social Security Numbers and Child Identity Theft

Robert Feldt
Special Agent-in-Charge, Dallas Field Division
Office of the Inspector General, Social Security Administration

September 1, 2011

Good afternoon, Chairman Johnson and members of the Subcommittee. It is a pleasure to appear before you, and I thank you for the invitation to testify today. My name is Robert Feldt, and I am the Special Agent-in-Charge of the Social Security Administration (SSA) Office of the Inspector General's (OIG) Dallas Field Division (FD), one of OIG's 10 field divisions across the country. The Dallas FD handles Social Security fraud investigations here in Texas, as well as in Arkansas, Louisiana, Oklahoma, and New Mexico. Today, we are discussing the Social Security number (SSN) and ways to improve SSN protection and guard against misuse and child identity theft.

Your Subcommittee has discussed this issue with SSA and OIG before, but with SSN use widespread throughout government programs and financial transactions, and technology constantly evolving, the threat of SSN misuse and identity theft persists. We in OIG are well aware of the central role that the SSN plays in American society, and part of our mission is to protect its integrity along with the other personally identifiable information (PII) within SSA records. To provide some context on the issue, in Fiscal Year (FY) 2010, SSA assigned 5.5 million original SSNs, issued 11.2 million replacement SSN cards, and processed more than 1 billion SSN verifications. The Agency also received about $670 billion in employment taxes related to earnings under assigned SSNs. Protecting the SSN and properly posting wages under SSNs is paramount to ensuring SSN integrity and protecting our citizens' PII.

While adults across the United States strive to protect their SSN and their identity to maintain a good credit rating, a correct earnings record with SSA, and accurate tax returns with the Internal Revenue Service, children are now becoming targets for identity thieves. At a recent forum on child identity theft sponsored by the Federal Trade Commission (FTC), experts estimated that more than 140,000 U.S. children are victims of identity theft each year. Experts pointed to a trend wherein identity thieves are targeting cyber attacks on schools and pediatric centers to obtain children's SSNs, which are valuable because a child generally receives an SSN at birth, but does not use it for credit purposes for about 18 years. This allows for the potential long-term undetected abuse of a genuine SSN—and the potential long-term harm to a young person's financial future.

We in OIG understand the concern your Subcommittee has for families and their children with regard to identity theft, and we pursue as many SSN misuse cases as our resources allow each year. In FY 2010, the Dallas FD opened more than 700 investigations based on allegations of violations including Social Security disability fraud, SSA employee fraud, and SSN misuse. Our FY 2010 investigative efforts in the Dallas FD resulted in the recovery of more than $3.2 million to SSA, and projected savings of more than $43 million in SSA funds. As we pursue SSN misuse and identity theft cases when possible, we have also made numerous recommendations to SSA and to the Congress to improve the SSN's security.

SSN Protections

As the Subcommittee is well aware, SSA created the SSN in 1935 to keep an accurate record of each person's Social Security-covered earnings. However, over the years, Federal and State governments have relied on the SSN as the identifier of choice for a variety of programs. Financial institutions are also required to obtain the SSNs of their customers. With each new use, the SSN has more value, and when you create something of value, inevitably someone will try to steal it. In May 2006, President Bush established the National Identity Theft Task Force, which created directives for Federal agencies to strengthen efforts to protect against identity theft. Our reviews have found that SSA has followed these directives for years and strives to improve SSN integrity.

SSA has implemented numerous improvements in its SSN assignment, or enumeration, process. We believe SSA's improved procedures have reduced its risk of improperly assigning these important numbers. Some of the Agency's notable improvements include:

- establishing enumeration centers that focus on assigning and issuing SSN cards;
- requiring that field office personnel who process SSN applications used a standardized Web-based process known as SSNAP, which reinforces Agency enumeration policies and standardizes data collection; and
- strengthening the requirements for identity documents presented with SSN applications.

In addition, to prevent misuse of personal information, SSA has reported the following actions:

- SSA removed SSNs from the Social Security Statement, displaying only the last four digits.
- The Department of the Treasury removed the SSN and other types of numeric identifiers from Federal checks.
- SSA no longer releases SSNs or any PII to a caller who cannot provide his or her SSN. SSA now refers such callers to field offices for further identity verification before releasing information.
- When SSA assigns a new SSN because a person has been harmed by the misuse of his or her original SSN, the Agency places a special indicator on the old SSN record to block issuance of replacement SSN cards and SSN printouts.

We in OIG have also spearheaded many efforts to protect and improve SSN integrity. For example, the work of OIG attorneys, auditors, and investigators led to the removal of SSNs from Selective Service mailings and the Thrift Savings Plan Website—two practices by which the Federal Government was itself putting the SSN at risk. We are also pleased to see that the Department of Defense (DOD) is replacing the SSN with a new DOD identification number on all identification cards, to protect the privacy and personal information of our military personnel and their families.

We applaud these and other efforts, but even now, SSA has no authority to prohibit the legitimate collection and use of SSNs. Nevertheless, our audit and investigative work has taught us that the more SSNs are unnecessarily used, the higher the probability that these numbers can be used to facilitate the commission of crimes throughout society. We believe SSA should support legislation to limit public and private entities' collection and use of SSNs, and to improve the protection of the information when obtained; continue its efforts to safeguard and protect PII; and develop appropriate authentication measures to ensure the highest level of security and identity assurance before offering replacement SSN cards over the Internet.

SSN Misuse Investigations

OIG's primary mission is to protect SSA programs and operations, and the majority of our investigations are related to SSA program fraud. However, our organization receives thousands of allegations of SSN misuse each year, and it is our experience that investigations into SSN misuse will often involve the elements of identity theft. At times, they can also involve Social Security fraud and can lead to the recovery of significant SSA funds.

For example, last year our El Paso, Texas office investigated the case of Mr. Elias Barquero. The investigation revealed Mr. Barquero used another man's SSN beginning in 1990, to assume the man's identity. He obtained a U.S. passport and a Texas identification card, and then applied for disability benefits. From 2001 to 2010, he fraudulently collected nearly $95,000 for himself, and nearly $48,000 on behalf of his two children.

Barquero's victim passed away in 2004, but Barquero misused his identity for almost 15 years. Authorities arrested him and charged him with theft of public money and identity theft. He was sentenced in October 2010 to two years in prison, and court-ordered restitution of more than $142,000 to SSA.

As we pursue investigations similar to the case of Mr. Barquero, our agents also participate on about 45 SSN misuse task forces throughout the country, which cover mortgage fraud, bankruptcy fraud, and document and benefit fraud, as well as identity theft. In FY 2010, we secured 441 criminal convictions based on our SSN misuse investigations nationwide.

Identity theft investigations have their share of challenges, as this crime takes on many forms; victims can have their name, birth date, and SSN stolen, and thieves can misuse the information in many ways. Also, there are many cases in which a person does not know his or her identity has been stolen. Therefore, if law enforcement learns an SSN has been misused, there exists the challenge of identifying and locating both the perpetrator and the victim.

Because jurisdiction over identity theft cases often overlaps, we have to determine who will investigate and prosecute the case. In fact, we investigate many of these cases jointly with other law enforcement agencies. Here in Texas, we have worked with the Austin County Sheriff's Office, the Harris County Sheriff's Office, the Texas Health and Human Services Commission OIG, the Texas Department of Public Safety, and the San Antonio Police Department. We have also worked with other Federal agencies, including the Department of Homeland Security's Homeland Security Investigations, the Federal Bureau of Investigation, the Postal Inspection Service, the Secret Service, and the Department of State's Diplomatic Security Service.

The proliferation of Credit Privacy Numbers (CPNs) is a relatively new SSN misuse scheme and a threat to the security of child identity information. CPNs are nine-digit numbers that resemble the SSN or the IRS-provided Individual Tax Identification Number or Employer Identification Number, but CPNs are a means of misusing the SSN and possibly committing identity theft.

Numerous unscrupulous agencies and organizations are providing CPNs—also known as Credit Profile Numbers and Credit Protection Numbers—for a fee, as a method of creating a new, separate credit file for individuals with low credit scores, bankruptcy, and slow or late payments on their current credit record. Websites offering CPNs advertise a new credit file with the use of a CPN, at costs ranging from about $40 to as much as $3,500. Despite what many of these credit repair Websites imply, consumers should know that CPNs are not legal; the only legal means of acquiring identification numbers related to credit is through SSA or the Internal Revenue Service (IRS).

According to the Identity Theft Resource Center, these credit repair companies appear to be targeting dormant SSNs, particularly those belonging to children, for reasons I have mentioned. However, there is no tangible evidence to indicate that children's SSNs are more vulnerable than the rest of the public.

Legislative Efforts

We support the prior bipartisan legislative efforts of this Subcommittee to limit the use, access, and display of the SSN in public and private sectors, and to increase penalties against those who fraudulently misuse the SSN. Most recently, the Subcommittee introduced the *Social Security Number Privacy and Identity Theft Prevention Act of 2009*. This legislation included new criminal penalties for the misuse of SSNs; criminal penalties for SSA employees who knowingly and fraudulently issue Social Security cards or SSNs; and enhanced penalties in cases of terrorism, drug trafficking, crimes or violence, or prior offenses.

The legislation would also expand the types of activities that are subject to civil monetary penalties (CMPs) and assessments under Section 1129 of the *Social Security Act*. Currently, an individual who misuses an SSN is not subject to a CMP, except in cases related to the receipt of Social Security benefits or Supplemental Security Income. The legislation would authorize the imposition of CMPs and assessments for activities such as providing false information to obtain an SSN, using an SSN obtained through false information, or counterfeiting an SSN.

The expanded use of the SSN in today's society has made it a valuable commodity for criminals. In addition to being a lynchpin for identity theft crimes, it also assists an individual to assimilate into our society, and in some instances, to avoid detection. The importance of SSN integrity to prevent identity theft and ensure homeland security is universally recognized. Providing enhanced, structured penalties is appropriate to reflect the vital importance of the SSN.

Reviews & Recommendations

Our ongoing and recently completed audit work has highlighted vulnerabilities and suggested some ways in which SSA can persuade public and private organizations to limit the collection, use, and disclosure of SSNs.

Regarding child SSNs, our report, *Kindergarten Through 12th Grade Schools' Collection and Use of SSNs*, released in July 2010, determined that many schools used SSNs as the primary identifier for students or for other purposes, even when another identifier would have sufficed. We believe that while some schools use SSNs as a matter of convenience, administrative convenience should never be more important than safeguarding children's personal information.

We have previously recommended that SSA seek legislation to limit SSN collection by State and local governments, and to limit access to SSNs by prisoners participating in work programs. In fact, our work on prisoners' access to SSNs preceded the President's signing of the *Social Security Number Protection Act of 2010*, which prohibited prison work programs from granting prisoners access to SSNs.

Additionally, although temporary residents may have authorization to work in the United States for the limited time they are here, we question the propriety of assigning an SSN, which is valid for life, to

these individuals, because the SSN may be a key to the temporary resident's ability to overstay his or her visa. We are working on or have completed related reviews on non-immigrant workers, noncitizens with fiancé visas, and exchange visitors.

Another issue to consider is SSA's procedures for issuing SSN verification printouts. Under the *Privacy Act*, individuals are allowed to obtain their SSN information from SSA, and the printout is among the items available. The printout is a limited version of SSA's Numident record, but it still contains the same basic information as the Social Security card. The printout, however, has no security features.

In response to the *Intelligence Reform and Terrorism Prevention Act of 2004*, SSA revised its policies for issuing Social Security replacement cards. Some of SSA's actions included increasing the identity requirements, such as presenting valid photo identification documents for obtaining a replacement SSN card; and limiting the number of replacement Social Security cards an individual can receive to no more than three in a year and 10 in a lifetime.

SSA's current disclosure regulations that implement the *Privacy Act* allow an individual to provide less probative identity documents to obtain an SSN printout. In certain circumstances, an individual can obtain an SSN printout from a field office without any identity documents. In a December 2007 report, *Controls for Issuing Social Security Number Verification Printouts*, we said procedures for issuing the printouts should follow SSA's improved replacement card procedures.

However, SSA did not implement similar procedures in the SSN printout issuance process. We will soon release a report that determined the Agency issued about 7 million printouts in FY 2009, up from about 4.6 million in FY 2003, the first full year SSA issued the printouts. We continue to believe SSA should strengthen its controls for issuing printouts. Since December 2007, we have found an increase in the occurrences of fraud involving printouts. We also measured the every SSA field office's printout output, and we found the 18 field offices located within 30 miles of the United States-Mexico border—including eight offices in Texas—did not generally issue a greater number of printouts than other field offices.

Citizens' Accountability

Identity theft, especially child identity theft, is serious, and while OIG and SSA have controls in place to protect the SSN, we should all be aware of the dangers of being careless with our and our children's personal information. We urge people to keep their and their children's Social Security cards in a secure place, to shred personal documents, and to be aware of phishing schemes, because no reputable financial institution or company will ask for personal information like an SSN via the phone or the Internet. It is also important to protect personal computers with a firewall and updated anti-virus protection.

Additionally, we should all be judicious in giving out an SSN in business transactions, because while it is required for some financial transactions, an SSN is not necessary for everyday transactions like applying for a gym membership or enrolling a child in piano lessons. It is also critically important that we all monitor our financial transactions regularly by checking credit reports from one of the three major credit bureaus. Concerned citizens may also contact SSA at 1-800-772-1213 if they suspect someone is using their SSN work purposes; SSA will review work earnings to ensure its records are correct. Anyone

who believes his or her SSN is being misused should contact the FTC at 1-877-438-4338, and he or she may also need to contact the IRS to address any potential tax issues.

Finally, we urge parents not to give their children their SSNs until the children understand how and why to protect the numbers. By knowing how to protect ourselves, and actually taking these important steps, we make life much more difficult for identity thieves.

Conclusion

SSA has a long history of protecting PII, and while current conditions may be the most challenging yet, we are confident SSA will rise to the occasion and address the challenges of today and tomorrow. Identify theft will undoubtedly persist for years to come, because of the reliance on the SSN as a national identifier and advances in technology and communication. Nevertheless, we are committed to ensuring that the information in SSA's records remains safe and secure. The SSN was never intended to do more than track a worker's earnings and to pay that worker benefits. However, as the use of the SSN has expanded over the decades, its value has increased as a tool for criminals, who are now targeting our children's personal information. Therefore, we must continue to ensure the integrity of the enumeration process; limit the collection, use, and public display of the SSN; encourage the protection of the SSN by those who use it legitimately; and provide meaningful sanctions for those who fail to protect the SSN or misuse it.

Our investigators are committed to pursuing SSN misuse and identity theft cases, and our auditors will continue to offer recommendations to safeguard the SSN. We will continue to provide information to your Subcommittee and Agency decision-makers about this critically important issue.

I thank you again for the opportunity to speak with you today. I am happy to answer any questions.

Chairman JOHNSON. Mr. Puente.

Mr. PUENTE. Good afternoon, Chairman Johnson and Members of the Subcommittee. My name is Antonio Puente and I'm a Special Agent in SSA OIG's Dallas Field Division working out of the San Antonio office. Thank you for the invitation to testify.

Identity theft is prevalent in Texas for several reasons. First, the Pew Hispanic Center estimates there are about 1.65 million unauthorized immigrants in Texas. These individuals may seek other's

personal information, like Social Security numbers, for reasons such as gaining employment and applying for government benefits.

Also, identity thieves have relatively easy access to other's personal information. Many fraudulent vendors offer stolen or fabricated identity documents for a fee. I want to share a recent identity theft case that my office and other law enforcement agencies investigated near Austin.

Last year, Pflugerville police learned that care takers in an area nursing home might have submitted false identity documents to gain employment. We verified SSNs of 43 employees suspected of submitting fraudulent personal information. The search revealed that 28 of the employees did, in fact, misuse an SSN. Twenty-three people were arrested. All of them pleaded guilty to buying a Social Security card from an unknown document vendor in the Austin area. In June, they were fined and sentenced to time served.

The Department of Homeland Security identified these individuals as Mexican nationals unlawfully present in the United States, and they are currently in deportation proceedings. Before this investigation, the nursing home did not use Homeland Security's eVerify system to determine the employee's eligibility to work in the United States. I met with corporate officials and provided instructions for using the eVerify system.

Also, the investigation revealed seven of 28 fraudulent SSNs belonged to children. The case shows that it's critical for parents to protect their children's Social Security cards and monitor their SSNs. In closing, I want to thank the many law enforcement agencies that contributed to this investigation, especially the Pflugerville police.

Thank you for the invitation to testify, and we'll be happy to answer your questions.

Chairman JOHNSON. Thank you, sir.

Mr. PUENTE. Yes, sir.

[The prepared statement of Mr. Puente follows:]

U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Field Hearing on Social Security Numbers and Child Identity Theft

Antonio Puente
Special Agent
Office of the Inspector General, Social Security Administration

September 1, 2011

Good afternoon, Chairman Johnson and members of the Subcommittee. It is a pleasure to appear before you, and I thank you for the invitation to testify today. My name is Antonio Puente, and I am a Special Agent with the Social Security Administration (SSA) Office of the Inspector General (OIG), working out of the OIG's Dallas Field Division, in the San Antonio, Texas office. Today, we are discussing ways to improve protection of the Social Security number (SSN) and to guard against misuse and child identity theft.

The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year. Identity theft is prevalent in Texas for several reasons:

- There are about 1.65 million unauthorized immigrants in Texas—the second-largest population in the United States behind California—according to 2010 estimates from the Pew Hispanic Center.
- Unauthorized immigrants in Texas, and across the United States, seek others' personal information like names, birth dates, and SSNs for many reasons, such as obtaining official identification documents, gaining employment, applying for government benefits, and opening financial accounts.
- Unauthorized immigrants seeking others' personal information—as well as all other identity thieves—have access to counterfeit identity documents, often through purchase from fraudulent vendors that have stolen or fabricated personal information.

To illustrate these issues, I want to detail a recent identity theft case that SSA OIG and several Federal, State, and local law enforcement agencies investigated near Austin, Texas.

In late 2010, the Pflugerville, Texas Police Department investigated a certified nurse's aide (CNA) at the Pflugerville Nursing Home and Rehabilitation Center, after a patient allegedly experienced a sexual assault. The investigation revealed the CNA gained employment at the nursing home by using a counterfeit Social Security card and Permanent Resident Alien Card. Pflugerville police took this information to the nursing home's corporate officials, who then conducted an internal audit of all of the CNAs employed at the Pflugerville nursing home. Corporate officials identified 43 employees who may have submitted suspect documents during the employment application process.

Pflugerville police then contacted SSA OIG and requested assistance in verifying the SSNs of the 43 nursing home employees in question. Our search revealed that 28 of the 43 SSNs did not match, meaning there were inconsistencies in names, birth dates, or SSNs. The searches found that seven of the SSNs were assigned to children, and five were assigned to deceased individuals. Moreover, SSA never assigned six of the unmatched SSNs.

Verification of the nursing home employees' alien registration numbers by the U.S. Department of Homeland Security (DHS) also revealed the numbers were valid, but they were not assigned to the individuals in this investigation. Analysis of the individuals' CNA license applications showed each individual provided a fraudulent or counterfeit Social Security card and Permanent Alien Card to the State of Texas.

We presented this information—documentation from the nursing home's corporate office, and results of the SSN verifications—to the U.S. Attorney's Office (USAO) for the Western District of Texas, Austin Division. The USAO opened criminal cases on all 28 individuals in November 2010. SSA OIG obtained arrest warrants, and a multi-agency arrest operation resulted in the arrest of 23 individuals, with five arrest warrants remaining open and active.

A Federal Grand Jury indicted the 23 individuals for SSN misuse and fraud and misuse of visas, permits and other documents. All 23 pleaded guilty to buying a Social Security card; they were each sentenced in June to time served and ordered to pay a $100 special assessment. DHS has identified all of the individuals in this investigation as Mexican nationals unlawfully present in the United States. DHS has processed the individuals, and each is currently in deportation and removal proceedings, with hearings pending.

SSN misuse and identity theft investigations may be criminally prosecuted, but they are more likely to be accepted for prosecution when they involve multiple or vulnerable victims with significant financial losses. According to the *Social Security Act,* criminal SSN misuse includes:

- Willfully, knowingly, and with intent to deceive, using an SSN assigned on the basis of false information provided by the individual or another person;
- With intent to deceive, falsely representing a number to be the SSN assigned to a person;
- Knowingly altering a Social Security card; buying or selling a card that is, or purports to be, a Social Security card; counterfeiting a Social Security card, or possessing a card or counterfeit card with intent to sell or alter it;
- Disclosing, using, or compelling the disclosure of the SSN of any person in violation of the law.

These are felonies punishable by imprisonment for up to five years and/or fines of up to $250,000. These penalties are separate from violations of other applicable statutes, such as immigration laws.

During this investigation, the USAO's victim-witness coordinator notified the victims that their SSNs were misused, but the victims in this instance were fortunate that the investigation did not reveal any specific harm. Our office worked with the USAO to provide this notification to victims; we also provided information on how they could review their credit reports and contact their respective local Social Security offices for additional assistance.

SSA has processes in place to assist victims of identity theft. SSA personnel will work with identity theft victims to:

- Review the earnings reported using their SSNs, and correct the record if necessary;
- Take an application for a replacement card, if the victim's Social Security card has been lost or stolen;
- Provide information to victims about the FTC-recommended actions a victim should take to remedy the effects of identity theft; and provide SSA information on identity theft, SSNs and Social Security cards;
- Take an application for a new, different SSN if the victim requests one and is able to provide evidence that he or she is being harmed by the misuse;
- Develop criminal aspects of the case if evidence shows fraud, and refer the case to OIG.

The individuals identified in our investigation purchased their counterfeit Social Security cards and Resident Alien cards from several unknown document vendors located in and around the Austin area within the last year. The vendors reportedly told the individuals that the SSNs on the counterfeit cards were randomly selected. None of the card purchasers provided the vendors' names or contact information to law enforcement.

Vendors that sell SSNs obtain the information through various means, including stealing identity documents or personal information, or carrying out online data breaches. Specific methods can include

simple dumpster diving, pick-pocketing, or stealing postal mail; or more recent schemes such as phishing and pre-texting—posing by e-mail or phone as someone who legitimately needs the information. In some cases, vendors simply randomly select nine numbers, because they are not concerned with the SSN's legitimacy; they simply want to produce a counterfeit Social Security card, so the purchaser is able to fill out a job application or open a credit account.

Before this investigation, the nursing home's corporate office did not use the DHS E-Verify system to determine the eligibility of their employees to work in the United States. SSA OIG met with the corporate council and provided contact information for DHS as well as instructions for using E-Verify.

Also, while this investigation involved a very small sample, we found that of 28 misused SSNs identified, 25 percent belonged to children. At a recent FTC-sponsored forum on child identity theft, experts discussed a trend wherein identity thieves are targeting cyber attacks on schools and pediatric centers to obtain children's SSNs. Therefore, it has become critical for parents to protect their child's number as they would their own, performing regular earnings records and credit checks on the child's number. In 2010, about 8 percent of identity theft complaints came from victims 19 and younger, according to the FTC.

In conclusion, the Pflugerville nursing home case was an excellent example of cooperation among Federal, State, and local law enforcement in an effort to curb SSN misuse and identity theft. The case highlights some of the current identity theft issues in Texas and across the United States. There is a critical need for U.S. employers to remain vigilant and to verify each employee's status as legally permitted to work in the United States using a correct and legitimate SSN. The case also illustrates the threat of undocumented vendors selling counterfeit SSNs and Social Security cards, either by stealing legitimate SSNs, in some cases from young children, or by selecting numbers at random.

I want to thank the many law enforcement agencies that contributed to the investigation: the United States Attorney's Office for the Western District of Texas, Austin Division; U.S. Department of Health and Human Services OIG; Federal Bureau of Investigation; U.S. DHS Immigration and Customs Enforcement (ICE) Homeland Security Investigations and ICE Enforcement and Removal Operations; Texas Attorney General Medicaid Fraud Control Unit; and the Pflugerville Police Department. We in SSA OIG are pleased to see this case successfully resolved, and we remain committed to pursuing similar SSN misuse and identity theft cases throughout the State of Texas and across the country.

Thank you again for the invitation to testify. I am happy to answer any questions.

Chairman JOHNSON. We're trying to push E-verify into all companies now, and I hope that makes a difference. I don't know if it will or not. Because they don't all use it right, you know that.

Mr. PUENTE. Yes, sir.

Chairman JOHNSON. As discussed, the time for each round of questions, I will limit my time to five minutes and ask my col-

leagues to also limit their questions to five minutes and any remarks that you care to make will be entered in the record.

Mr. Bryson and Ms. Lanius, were either of you aware of the crime of identity theft when you or your family became victims?

Mr. BRYSON. No, sir, I was not.

Ms. LANIUS. No.

Chairman JOHNSON. And had you heard of any precautions that you needed to take to protect your family's Social Security number.

Ms. LANIUS. No.

Mr. BRYSON. No.

Chairman JOHNSON. No one advised you of that? Did both of you know where to go for help once you knew it occurred?

Mr. BRYSON. No.

Chairman JOHNSON. How did you find out, either one of you?

Ms. LANIUS. I talked to the police and they told me there's really nothing that could be done because I had to prove I hadn't made those purchases. And I drove, because back then there was no Internet, to all the credit bureaus, and I had to drive to all the vendors begging them to stop reporting these purchases under my Social Security.

Chairman JOHNSON. And they wouldn't help you?

Ms. LANIUS. No one would help, no. The burden was on me and no one—no one would help. There was no place to go.

Chairman JOHNSON. Do the credit guys help now?

Okay. Thank you, Ms. Lanius. What did you do finally to prove that you didn't make these purchases? How did you finally get out from under that?

Ms. LANIUS. I did not. I could only circle the items on the credit report that I was claiming were fraudulent. The credit agency at that time would put a note under those saying that the person—the account had claims this was a fraudulent purchase, but they still stayed on my report for seven years, and it still went into my credit rating for seven years. And that was the only thing I could do. I did speak to the doctor's office who called me to collect on a surgery she had had.

Chairman JOHNSON. Wow.

Ms. LANIUS. And they said all I could do was go in and prove by examination that he hadn't operated on me, and I was wasn't going to do that. So the surgery went on my credit history as well.

Chairman JOHNSON. That's almost insurmountable. I don't understand that.

Agent Feldt, would you explain what steps Social Security employees are instructed to take to help victims?

Mr. FELDT. Yes, sir. SSA has processes in place to assist victims of identity theft. SSA personnel will work with identity theft victims to do several things. First, SSA will review the earnings reported under the SSNs and correct the record, if necessary.

Chairman JOHNSON. Well, but in her case they didn't do it. Was Social Security not working at that point in time?

Mr. FELDT. These policies were probably not in place at that time.

Chairman JOHNSON. Okay.

Mr. FELDT. That's correct.

Chairman JOHNSON. So you're saying this couldn't happen again.

Mr. FELDT. I would not be bold—so bold as to say that.

Chairman JOHNSON. Okay.

Mr. FELDT. They also have a few other procedures in place to help individuals if they've lost a card to retain a replacement card, and also to provide information to victims about the FTC and help they can provide. Also, although it's not an item that's used very often, they will take an application for a new Social Security number. However, the victim must prove they've been harmed in that situation.

It is frowned upon to do that because ultimately if that—if that step is taken, the Social Security numbers and the record will come together in time through the credit bureaus. So that's not very effective and it's discouraged. And lastly, employees will develop aspects of fraud in the matter and potentially refer it to the OIG for investigation.

Chairman JOHNSON. Thank you.

Mr. FELDT. Yes, sir.

Chairman JOHNSON. I think my time's expired.

Mr. BRADY. Chairman, thank you very much for holding this hearing. For the audience, from the first day I got to Congress, Chairman Johnson was an early and very vocal proponent regarding our Social Security ID numbers and shining a light on identity theft, so thank you. I had no idea the amount of child identity theft was occurring before you scheduled this hearing and as a parent to young boys, I'm more nervous than ever as a result.

One of my frustrations on this committee and on these hearings has been how rare it is to—for an identity thief to be apprehended and prosecuted. It seems each week I pick up the newspaper, I see prosecution of Medicare frauds, securities fraud, consumer fraud. I can't remember the last time I saw a report of identity theft actually have been prosecuted.

Ms. Lanius and Mr. Bryson, you both contacted law enforcement, I assume not satisfied with the result of that contact. So I wanted to ask Ms. Kueckelhan and Mr. Feldt, you know, give us perspective. What are the chances in America that an identity thief will be apprehended and prosecuted?

Ms. KUECKELHAN. Congressman Brady, I can say the Federal Trade Commission, since 2001, has brought 34 data breach law enforcement actions and that is where massive breaches of Social Security numbers have occurred. And we will continue to bring those types of law enforcement actions.

I'm also pleased to mention that we have brought the first mobile app misrepresentation case, filed on August the 15th. It's the first such case that a federal agency has brought. We brought it against a mobile app provider who obtained children's information and used that information and distributed it without the parents' consent.

So we in our law enforcement area, if you're asking about that, we work more from the data breach than the bigger perspective. We also provide education and support to legal aid entities who represent ID theft victims. The FTC provides them with sample affidavits and letters, assistance on what to do, what steps to take.

Mr. BRADY. Can I ask you, in these cases, there wasn't a data breach, so the Federal Trade Commission would not—is not or would not be pursuing cases that affected Ms. Lanius and Mr. Bryson.

Ms. KUECKELHAN. We do not represent one individual in a private case. For a misrepresentation case, we look for a pattern and practice and that's why we take on the large data breach cases. Generally speaking, individual ID theft victims are assisted by legal aide representatives. In addition, the FTC provides consumer materials and online information for self help, including assistance with affidavits and letters.

Mr. BRADY. Mr. Feldt.

Mr. FELDT. Yes. We—as far as challenges, there's——

Mr. BRADY. What are the chances in SSA's view that someone who commits this crime will be apprehended and prosecuted?

Mr. FELDT. We work cases every year as an organization in which folks are apprehended.

Mr. BRADY. And I'm not being—I'm just trying to get a perspective.

Mr. FELDT. Yes, sir.

Mr. BRADY. Would it be fairly rare.

Mr. FELDT. I don't know what the percentage would be of allegations of SSN misuse that actually result in a conviction. But I would agree with you that it would be—it is rather rare. There's a lot of misuse of Social Security numbers going on that ultimately is not prosecuted.

Mr. BRADY. What more can be done? Clearly Congressman and Chairman Johnson focus on prevention early on in protecting the integrity of these numbers, but, you know, what needs to be done? New laws? New resources? I don't know.

Ms. Lanius, did they ever apprehend this Stacey Rogers?

Ms. LANIUS. No.

Mr. BRADY. Never. Did they—Mr. Bryson, any of the six or seven or eight, do you know of——

Mr. BRYSON. No, sir.

Mr. BRADY. What do we need to do.

Mr. FELDT. Number one, doing anything we can do to prevent the disclosure of Social Security numbers and any enhancements that can be made, we would support. And additional resources can always help. To have more feet on the ground to investigate identity theft, would be a good thing.

Actually, so many of the cases that are prosecuted, they will start at the local level in which they start with a local complaint to a police officer, and then you have jurisdictional issues in many times. And we get referrals from local police offices and at the local level that many times result into federal convictions.

Mr. BRADY. Dr. Vieraitis, did the folks that you interviewed, did they—as they were committing the crime, did they think they were gonna get away with it?

Dr. VIERAITIS. They were very confident in their abilities and they thought they would get away with it. And even though we spoke to people who were sitting in prison, so clearly they did not get away with it, they blamed their capture on outside things they deviated from the plan, dumb luck on the part of law enforcement,

or they were working with others who got caught up in the trafficking.

Mr. BRADY. The times I—and I appreciate that, FTC, Social Security ID, get frustrated. I wish we'd spend a little less time pursuing celebrity sports cases and a little more time as a government focusing on identity theft. I think we'd actually help a lot more people.

Ms. KUECKELHAN. Congressman Brady, the Federal Trade Commission has civil authority. We have no criminal authority.

Chairman JOHNSON. Well, that's true, so can you answer the question for me: How many of those cases were children below the age of, let's say, 18.

Ms. KUECKELHAN. The data breach numbers?

Chairman JOHNSON. Yeah.

Ms. KUECKELHAN. I don't have those numbers. And also, it's important to note on the 192 percent that you stated, Chairman Johnson, although that is an accurate percentage of the increase in child identity theft complaints for which the person reporting completed the field that ask for the victim's name, many consumers do not disclose the victim's age. Therefore, that is not based on a scientific survey. It is instructive, but not scientific.

On our complaint system there is a field that ask for the child's age at the time that they were victims. Many of those that report do not include an age.

Chairman JOHNSON. They don't fill it out.

Ms. KUECKELHAN. No, sir.

Chairman JOHNSON. How about, Feldt, do you know what percentage are under the age of 18 when they're stolen.

Mr. FELDT. I'm sorry, I do not know the number. We can sure get that back to you.

Chairman JOHNSON. We give SSNs to them when they're born nowadays for goodness sake and I'm telling you, I don't know of a baby in the world that's gonna go and check his credit.

Ms. KUECKELHAN. Chairman Johnson, of those that did report an age in 2010, over 24,000 were under the age of 19.

Chairman JOHNSON. Okay. Well, that's a good statistic. Thank you very much. Mr. Marchant.

Mr. MARCHANT. Thank you, Mr. Chairman, for the opportunity to participate in this hearing. I have a formal statement I'd like to submit to the record. I also would like to submit to the record a Wall Street Journal story that was written this week, August 27, about a family in Dallas who had had their children targeted by identity thieves. So it's a very timely article, and it's about a local family.

What got me interested in this was a case that came into our congressional office about a family who had applied for this Social Security card for an infant, a new-born infant. And I know my son, when his children were born, he—one of the first things he did was he applied for a Social Security card. And this family that I represent applied for their Social Security card.

And after a while, they had not received it so they began to look into why they had not received it, and then they were contacted by the police who were doing a very good job, and they notified them that, in fact, the Social Security card had been removed from their

box out in front of their house. So they were harvesting the mail in this neighborhood.

They got the Social Security card. They began to use it. And only through that mechanism did this family find out not only, you know, here's why you didn't get your card; but that's one bad news. The next part of the bad news is your child was already very deeply in debt and has a very bad credit rating, even though they haven't achieved their first birthday.

So we began to work on some legislation. With the Chairman's permission, we will pursue the legislation when we get back to Washington. And the objective of our legislation will be, first of all, to come up with a more secured delivery system of that first Social Security number. I think that in itself would cut down a lot of the abuse and fraud of not putting that in the mailbox when we have the ability to get a secure number over the Internet. There are a lot of ways to secure this valuable number without having it put in your post office box.

The second thing we would like to accomplish is when you have a card issued to an infant and if it's brought to the Social Security Administration's attention that that has already been stolen and compromised, there needs to be a standard process of issuing a new number to that infant or child. There also needs to be a standard system where that old number goes into the Social Security system and is flagged. And if there's any activity on that number, any income activity, a big red flag needs to just pop up. And you'll have an immediate printout of here of your fraud cases.

I mean, that to me, that is just a mechanical process that can be done. Then I think you can come to Congress and say, okay, here's our list. Give us the boots on the ground to just go enforce this law. I don't see any mechanism on the books now to even to accomplish this process. So we're gonna try to help you with permission from the Chairman. We're gonna try to help you with that system.

And then I think that we have to notify parents somehow or another when they apply for a card for a minor, they need to get some immediate information back from the Social Security Administration. When they get that number, they need to immediately be apprized of the problems that they're going—that they can have and the importance of it.

It's almost a gift to the criminal world the way that we operate this system. And if there was somebody in this audience today that was trying to learn how to easily get into this system, I think they have a pretty clear roadmap of how to do it. They have a pretty clear roadmap of the very rare odds of them being apprehended and how very lucrative this can be.

We can do this. We've got super computers. We've got dedicated people in the field that are willing to enforce this. We've got parents. We've got agencies who are willing to solve this. I think it's incumbent on our Committee, Mr. Chairman, to give them the tools and the direction they need.

Chairman JOHNSON. Thank you. I think we're looking at that for starters—why do we give babies at birth a Social Security number? I'm kind of in favor of stopping that. We've discussed that a little bit yesterday.

Mr. FELDT. Yes, sir.

Chairman JOHNSON. Thank you. Dr. Vieraitis, you've done some interesting work in reviewing ID theft criminals and from that research, what approaches did they use to commit the crimes?

Dr. VIERAITIS. How much time do I have.

Chairman JOHNSON. Not too much. Try to synthesize it.

Dr. VIERAITIS. All the ways that you hear about, they use. They will steal from mailboxes. They will target dumpsters outside businesses such as insurance companies or schools that don't properly dispose of their data or files. They pay company employees, American Express or Visa or home mortgage companies.

They work with other street offenders who are involved in drug sales who know drug addicts who are willing to sell their own information in exchange for money.

Chairman JOHNSON. Well, when you say they pay employees of American Express or Visa or somebody, what do you mean?

Dr. VIERAITIS. They just happen to know someone who's working there. In exchange for money, the employee will give them information of people in their data base.

Chairman JOHNSON. So those credit companies have been cooperative.

Dr. VIERAITIS. There have been employees of credit companies, yes, that have sold information.

Chairman JOHNSON. Have you run into that.

Dr. VIERAITIS. Yes.

Chairman JOHNSON. Mr. Feldt.

Dr. FELDT. Yes, sir.

Chairman JOHNSON. Okay. Well, where do you think that we might go next to try to stop this other than stopping a number at birth.

Dr. VIERAITIS. I think that the FTC has done a fabulous job educating consumers and potential victims on how to protect their data. I don't know if the majority of people get that information. There are probably people who simply don't know and aren't aware of it. So constantly increasing awareness of it and encourage people to report.

People don't report to law enforcement; and if people don't report to law enforcement there's not as much we can do if we know about all of it. Most people ?? and I know this doesn't apply to you. Your cases were more severe. Most people resolve it within one day because most of it has to do with credit card fraud and the fraudulent use of credit cards.

So the good news is that for most people it's fairly easily resolved, and it's gotten much better and faster to resolve because of policies of the FTC and also Congress passed major legislation, for example taking credit card numbers off of receipts and other things like that.

Chairman JOHNSON. When you find out somebody in a credit card company is doing that kind of thing, do you report it to the authorities?

Dr. VIERAITIS. The company should report it to the authorities.

Chairman JOHNSON. But are they doing it?

Dr. VIERAITIS. I don't know.

Chairman JOHNSON. How do they find out? How does the company find out if someone's——

Dr. VIERAITIS. Through law enforcement investigations.

Chairman JOHNSON. So they can go a long time without finding out about it.

Dr. VIERAITIS. Yes, they could.

Chairman JOHNSON. Okay. Thank you very much. Ms. Kueckelhan, what legislation could we pass to stop ID theft in general, but children's ID theft in particular? And you know we're looking at trying to stop the hospitals from giving them at birth. Would that help you think?

Ms. KUECKELHAN. Chairman Johnson, may I address the doctor's comments about the——

Chairman JOHNSON. Sure.

Ms. KUECKELHAN [continuing]. About the theft with the companies.

Chairman JOHNSON. Please do.

Ms. KUECKELHAN. The Federal Trade Commission has the red flags rule, and the red flags rule is—one of the requirements is that a company develop internal standards of data security, in other words, minimize access within. And there's a variety of steps that's recommended that businesses take. So the red flags rule if a company, if it applies to them— it doesn't apply to every type of company. Some are exempt. But that would help to set measures in place. Again, not 100 percent full proof, but it should help in that regard if companies did follow it.

The Federal Trade Commission has previously recommended changes in the National Consumer Authentication Standards. Just as you stated, Congressman Johnson, SSN is used across the board as an identifier. Following suggestions from our forum, we'll continue to look at child ID theft issues that we should work with Congress on for changes.

Chairman JOHNSON. Thank you.

Mr. BRADY. Now, Ms. Kueckelhan, thank you for I understand FTC's very informed forum on the emergent problem of child identity theft, so I appreciate you bringing those experts together and those folks. You know, I want to ask you a question and I want to ask Dr. Vieraitis and Mr. Feldt follow-up on Chairman Johnson's question about what changes in law does Congress need to make to either protect people from identity theft or create more tools to apprehend and prosecute.

But from the FTC standpoint, do you publicly identify companies that are more prevalent in allowing their data to be breached or—where there are red flags that occur on a regular basis? Do we as a public, are we privy to the information about which companies do a poor job or are more likely to be—our identity is more likely to be breached with doing business with them from a transparency standpoint?

Ms. KUECKELHAN. I don't know that it's a transparency issue, but unlike an entity like the BBB that has ratings and reports online that would be available to the public; when a consumer files a complaint with the Federal Trade Commission, that is confidential as to the public. The public doesn't have access.

But we do open and welcome other law enforcement agencies to become—have the right credentials to access our database system so that we are the repository for many complaints and ID theft being one of those types and accessible to all so that even when the criminal authorities working on the individual identity theft side, they have access to our database.

Mr. BRADY. If it's a government agency whose data is breached or government officials who are selling those or providing the information for thieves, who handles those types of cases?

Ms. KUECKELHAN. I'm not sure I understand your question.

Mr. BRADY. You pursue on the civil side when companies have data breaches that are potentially dangerous for identity theft. So who pursues those when it's government agencies that the data's breached or employees are providing that information.

Ms. KUECKELHAN. Well, from the consumer's perspective, the misrepresentation takes place when a company represents that their security policies have certain qualities that they don't and that misrepresentation gives rise to our authority in the Federal Trade Commission Act.

Mr. BRADY. Dr. Vieraitis and Mr. Feldt, what can Congress do to help better protect individuals, and what needs to be done to significantly increase the prosecutions?

Mr. FELDT. I'd be happy to speak first. Any legislative provisions that would limit the collection, use or disclosure of Social Security numbers would greatly help our efforts.

Mr. BRADY. But Chairman Johnson's legislation would be a good place to start.

Mr. FELDT. Exactly it's a very good place to start; as well as enhanced penalties. As your studies have found, the risk just appears to be worth taking for these sophisticated criminals. Some of——

Mr. BRADY. Do you know what these punishments range?

Mr. FELDT. Well, for a first time offense, it potentially could be a six month probation or up to a year in prison. But we're not talking about four, five, six years in prison for many white collar crimes.

Ms. KUECKELHAN. Congressman Brady, on the civil side when we have pursued those statutory wrong on the civil law enforcement against companies that misrepresented their set—security policies, we have ratcheted up the so-called merchant provisions and some of those are up to 20 years.

Mr. BRADY. On the prosecution criminal side, where there is low risk of apprehension and prosecution and you're saying that the penalties aren't very stiff for——

Mr. FELDT. For first offenders. As you spoke about, many are first time offenders and without, you know, a major criminal history on the federal side, typically, the penalties are not great for——

Mr. BRADY. Doctor, what kind of sentences were there for those you interviewed, and what were their sentences?

Dr. VIERAITIS. Those we interviewed ranged from a minimum of 12 months to 30 years.

Mr. BRADY. Were they first time offenders generally?

Dr. VIERAITIS. Some of them were first time offenders and they did receive a significant penalty. They all thought that they would

get much less and most perceived the penalty would be probation, and they were hit much harder than they thought. So there's a perception——

Mr. BRADY. Because these were federal prosecutions?

Ms. VIERAITIS. Likely because they were federal prosecutions. Local prosecutors sometimes kick them up to the feds because they have more resources or it's a federal crime. It's crossed states lines. There are a lot of issues with jurisdictions. It makes it very difficult for law enforcement to take the report and also do something about it.

But any legislation that will reduce the use of Social Security numbers on Medicare cards, Medicaid cards, foster children would certainly help; but I would like to say that in terms from the offender's perspective, the riskiest part for them of that whole crime is walking into a bank or walking into a store and cashing in on it.

So getting the number is easy; but the riskiest part for them, the one that causes the most stress and the part where policy would be good to target, is making it impossible for them to cash in on it. And the credit card companies and the businesses have but need to do more to protect consumers from that.

Mr. BRADY. Any chance of that risk go down even more if they steal a child's Social Security number?

Dr. VIERAITIS. I think the eVerification system and any system that can alert the credit card company, the bank, anywhere you're trying to use it that says this number belongs to a person under the age of 18, and the person applying for it claims that they're 40. It doesn't match up. Some sort of system.

And I believe this was brought up at the FTC conference this summer. Some sort of verification to link that number to a child so that the offender can't use it to apply for a home loan because no 12-year-old is applying for a mortgage.

Mr. BRADY. Well, not as many anymore prior to 2008. But we fixed that so. Chairman, I went over time.

Chairman JOHNSON. That's all right. Thank you, Mr. Brady.

Mr. MARCHANT. During the last year, we at our congressional office has become very proactive in going into senior centers and going into libraries and having identity theft seminars. We thought that maybe 20 people would show up. Sometimes 20, 30 people show up in that kind of seminar. We are having incredible turnouts. And we appreciate the help that we have received from several of the agencies in doing this. We're having hundred, 120 people show up at these identity theft seminars. So it's a big issue.

And the people that are most afraid of it now seem to be the seniors. And I'm beginning to detect that maybe we should have a seminar or public meeting with young families and young couples and begin to tell them before they have a teenager, what's happening to you folks has happened.

So the other thing that I would request from all the agencies is a liaison, a specific liaison person that the 535 members of Congress have so that we have this kind of a case coming into our office that we will be able to say, okay, we can call this person at these agencies and get a direct liaison and get a very practical step-by-step thing that we can do to help that constituent because

by the time we get to talk to constituents, many times they are very frustrated. A lot of the damage has already been done. And we feel very frustrated when they come to us and everything's happened and the police have said there's nothing we can do. The District Attorney in many instances has said there's nothing we can do. And by the time they get to us, they're pretty frustrated. So if we can have a direct person that we could contact, it would be very helpful.

And then again I'd like to thank the agencies that have come out and help us with our identity theft seminars. They are very popular and for the first time we feel like we're trying to make people aware.

I would like to ask Mr. Puente, when you go out and you have a case in your hands, is there a typical offender that you will find when you get out the case in your hand?

Mr. PUENTE. Yes, sir. And just so you'll know, my area of responsibility runs all the way down the Rio Grand Valley, so from Brownsville all the way up to Laredo and Corpus, the San Antonio area. So typically I'm looking for individuals who are undocumented aliens; and when I have an identity theft case in hand, that's the first place I start.

In most cases, and I've been doing this almost 10 years, the trends that I've seen in Texas that have shifted towards U.S. citizens selling their documents to the document vendors, the parent selling their children's documents. And these undocumented aliens are buying these documents in Mexico because it's cheap.

Another thing that I have found is some document vendors are just making the nine-digit number up. Everybody knows that the Social Security number is nine digits. It doesn't matter what it starts with or it ends with; but everybody knows that you have to have that nine-digit number to get a job, to get an ID, to get a credit card. Everybody knows that.

And in the case that I worked in Austin, all the defendants that we debriefed, they said the same thing: I didn't care what it looked like as long as it had nine digits and I could get a job. And they were paying $50 to $100 in a flea market in Austin. So that's what I'm looking for.

Mr. MARCHANT. Okay, thank you.

Chairman JOHNSON. So what you're telling me is this number that the IRS gives out, which is nine digits, for people who don't have a Social Security number or ID, it wouldn't matter to the vendors down there.

Mr. PUENTE. No, sir. In fact, in this particular case, we had two of the defendants that actually had a tax ID number that they were using.

Chairman JOHNSON. As a Social Security number.

Mr. PUENTE. Yes, sir. They had counterfeited a Social Security card with that tax ID number on that Social Security card.

Chairman JOHNSON. Well, how is that getting through the system?

Mr. PUENTE. The facility that they were working at did not verify any of the Social Security numbers, any of them. So these employees were just able to fill out applications.

Chairman JOHNSON. So using E-verify might work to stop that?

Mr. PUENTE. It does work. It absolutely works, yes, sir.

Chairman JOHNSON. Mr. Brady has one more question.

Mr. BRADY. Well, one, I wanted to thank you Chairman for holding this hearing. This is obviously a problem growing by the minute and it's critical that we're aware of it. Secondly, these panelists have really given us great insight and I want to thank you for that. For the parents in the crowd today and parents learning about this problem, can I ask, what is the one or two most important things we can do to protect our families and our children from identity theft?

VOICE. Don't give out your number.

Chairman JOHNSON. Don't everybody speak at once.

VOICE. When you're asked to give your Social Security number, refuse to give it.

Mr. BRADY. Can I ask our panelist from your studies and prosecutions and interviews, what can we do as parents?

Dr. VIERAITIS. I would agree with what he just said. I don't memorize my daughter's security numbers. I don't carry their cards with me, and I never give the numbers out, ever. There are always blanks on forms for it and I just refuse to give it out. And also check. I know if you call a credit card company and run the number, it might not pop up. It will pop up 'file not found', but that doesn't mean it's not being used.

I would imagine the Social Security Administration would be—Mr. Feldt—would be the place that you would need to check. If you're concerned about it, check.

Chairman JOHNSON. Thank you, Mr. Brady.

Mr. BRADY. Thank you, Chairman.

Chairman JOHNSON. Again, I want to thank y'all for being here, especially Ms. Lanius and Mr. Bryson for sharing your personal experiences. Thank you so much. I also appreciate hearing the views of those of you on the front lines fighting identity theft, Ms. Kueckelhan and Feldt and Puente. And Dr. Vieraitis your testimony is the first time the Subcommittee has had an opportunity to examine the crime of identity theft from the thieves themselves. Thank you for your important research. And all of your testimony will help us do what's right to stop the misuse of Social Security numbers and prevent identity theft.

We're gonna work the problem, and I can tell you that all three of us are interested in resolving it and making this great America a better place for all of us to live. Thank y'all for being here. The committee is adjourned.

[Whereupon, the subcommittee was adjourned.]

Member Submissions For The Record:

U.S. Congressman Kenny Marchant
Committee on Ways and Means Opening Statement
September 1, 2011

I would like to thank Chairman Johnson for hosting this hearing on Social Security numbers and child identity theft. Thank you, also, to Mayor Dyer and the Plano City Council for graciously allowing us to hold this hearing in your chambers. Thank you to the scouts, too, for their wonderful presentation of the colors.

The figures on Social Security numbers and identity theft are alarming. According to the U.S. Department of Justice, between 2006 and 2008 approximately 11.7 million Americans were victims of identity theft. This takes a huge toll on the economy. The Federal Trade Commission reports that identity theft costs American consumers around $50 billion annually. Many of these stolen identities come from Social Security numbers. Some of the most vulnerable to identity theft are children. The FTC points to 19,000 cases of child identity theft reported in 2009, an almost 200 percent increase since 2003. A recent Carnegie Mellon University study says that child identity theft during 2009 and 2010 took place at a rate 51 times higher than the rate calculated for adults.

U.S. Congressman Kenny Marchant
Committee on Ways and Means Opening Statement
September 1, 2011

The question today, then, is whether we move in the direction of protecting Social Security numbers and combating rampant identity theft – particularly of children – or in the direction that simply looks the other way. I think the direction we should take, to shield individual security and fight child identity theft, will depend in part upon the knowledge and action gained from hearings like this.

We discuss today an issue that hits close to home. Not long ago, a constituent from my district had her then six-month-old son's Social Security card stolen by a convicted felon. The child's Social Security card was removed from the family's mailbox without their knowledge. Later, a local police department recovered the child's stolen Social Security card among a pile of other private information from the perpetrator. The police department notified the child's mother of the theft, and that the thief had a long history of forgery, credit card abuse and identity theft. In other words, the six-month-old child's identity had been compromised before the family had even received the Social Security number.

U.S. Congressman Kenny Marchant
Committee on Ways and Means Opening Statement
September 1, 2011

The police department's diligence should be applauded, but the larger point remains that identity theft of Social Security numbers impacts all Americans, of all ages, of all backgrounds, and in all parts of the country. This week's *Wall Street Journal* tells the story of a Dallas woman who was almost denied state medical benefits for her children when she learned that her one-year old daughter had apparently been earning income – and that the one-year old had amassed $39,000 worth of debt. Thieves cover and exploit Social Security numbers – especially, as in this case, an innocent child. Therefore, it the duty of this subcommittee to ask: Are we doing as much as we can do to protect Social Security numbers? If a child, or any American, has their Social Security number seriously compromised, what steps is the Social Security Administration taking to protect the individual's identity? What more can be done?

If a child has their identity number compromised, there should be practical steps to flag the old number and get a new, secure number. That is why when Congress returns to Washington, I plan to introduce legislation that proposes to do just that. But that is just a start. We must do a better job at protecting all Social Security identities, of the young, old, and in-between. That is the obligation upon this committee, and one that I am pleased the chairman and those here today take seriously.

Submissions For The Record:

Axton Betz

Contact Information:

Axton Betz
Assistant Professor of Consumer Studies
School of Family and Consumer Sciences
Eastern Illinois University
600 Lincoln Avenue
Charleston, Illinois 61920
Voice: (217) 581-2164
E-mail: aebetz@eiu.edu

This statement should be attributed to Axton Betz.

Statement for the Record of Field Hearing on Social Security Numbers and Child Identity Theft

The recent research, legislative, and media attention given to the problem of child identity theft is long overdue[1]. The recent attention to this problem has primarily focused on SSN-only identity theft. Many child victims of SSN-only identity theft have a parent or guardian discover the identity theft while they are still a minor. This attention has ignored a population of child identity theft victims who had their identity stolen while a minor, but did not learn of the crime until they were a legal adult. These victims, adult/child identity theft victims[2], endure a long, frustrating road to recovery as typically by the time the crime is discovered, their identity has been used for a number of years to establish a variety of fraudulent accounts.

Compounding the frustration for adult/child identity theft victims is that they often lack the consumer education and experience necessary to navigate the complex network of institutions and agencies that are supposed to assist them with their recovery, including banks, police departments, credit reporting agencies, health insurance agencies (for medical identity theft), and others. Additionally, often agencies do not work together in supporting an adult/child identity theft victim's recovery leaving the victim confused in how to proceed with regaining their identity. While in the process of recovery, which can take a number of years, adult/child identity theft victims often learn to "do without" as they begin their adult lives. For example, there have been adult/child identity theft victims who were unable to obtain student loans so they

[1] Power, R. (2011). Child identity theft: New evidence indicates identity thieves are targeting children for unused social security numbers. Retrieved September 14, 2011, from http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf

[2] Foley, L., & Nelson, C. (2009). *ITRC fact sheet 120: Identity theft and children.* Retrieved March 22, 2010, from http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_120.shtml

had to postpone their post-secondary education[3]. Other adult/child identity theft victims have had difficulty establishing utilities in their name. For those who have been fortunate enough to establish credit in their name, many have been required to pay additional deposits and exorbitant interest rates.

Adult/child identity theft victims often face significant financial obstacles; however, the troubling effects of identity theft extend to the victim's personal relationships. Often, friends and relatives are unable to be supportive of the adult/child victim's recovery simply because they lack an understanding of the multiple issues the victim is facing. This lack of support is further amplified if a relative or friend is the perpetrator of the crime, which is often the case in instances of identity theft.

Identity theft can affect the core of a person's emotions, including trust. Development of feelings of trust is central to an individual's healthy emotional development[4]. Adult/child identity theft victims often experience a loss of a sense of trust and this often has a negative impact on a victim's familial, social, and professional relationships. Many victims, especially those who never learn the identity of the perpetrator, don't know who they can trust: After all, anyone they know could have committed the crime.

My preceding comments are enlightened by both a research background in adult/child identity theft and personal experience as an adult/child identity theft victim. My current research examines the experience of recovering from adult/child identity theft. A previous research project explored consumers' perceptions of identity theft[5]. My experience as an adult/child identity theft victim (and subsequent adult victim of identity theft due to a data breach) have informed my research.

My adult/child identity theft experience was unique in that my parents' identities were stolen at the same that mine was stolen, when I was 11 years old. From the time I was 11 years old until the time I discovered I was a victim of identity theft at the age of 19, I watched my parents try and seek help from agencies and organizations including the local police, utility companies, creditors, and the post office along with many others. The assistance provided by these agencies and organizations was minimal at best. Oftentimes my parents were told "Sorry, there's nothing you can do about this."

---

[3] Betz, A.E. (2007, November). *Living with my invisible shadow: The experience of being a child identity theft victim in central Iowa*. Poster session presented at the Iowa State University Extension to Families In-Service. Ames, IA.

[4] Thomas, R.W. (2005). *Comparing theories of child development* (6th ed.) Belmont, CA: Thomson.

[5] Betz, A. (2009b). The effects of demographics on consumer perceptions of identity theft in rural and urban settings. *Consumer Interests Annual, 55*, 9-27.

It is difficult to capture all of the problems my parents encountered during these years, so the following paragraphs detail some of the more memorable incidents related to the theft of their identities:

One day my father brought me home from school and there was a yellow door-hanger attached to the front door; it was from the electric company. Our service had been disconnected due to non-payment. My parents had paid our bill, but someone had established electric service in their name and hadn't paid the bill so our electricity had been shut off. I did my homework by flashlight that night.

On a different day, a sheriff's car pulled into our driveway. I happened to be the first person in the house to notice it. After saying something to my parents, my father told my mother and me to hide. He went out to see what the sheriff's department wanted: They wanted to arrest my mother for check deception. Based on the information the sheriff's department had, my mother had been passing bad checks at the local Wal-Mart. It wasn't her; it was the identity thief.

Several semesters after I had left for college, I received notification from the university that the check my mother sent in for that semester's tuition had bounced. I knew this couldn't be true as my parents have the personal financial management skills to avoid bouncing checks. I was very angry over the situation and convinced it was in error, so I went to the appropriate university office and proceeded to tell them that this had to be an error. They were insistent that they were right, so insisted to see a copy of the check that had bounced. They were able to produce a copy of the check. The check looked exactly like my mother's—her contact information, her financial institution information, her check design—but the handwriting on the check was not hers. An identity thief had checks made to look exactly like my mother's, stole my tuition bill out of the mail, and wrote a fraudulent check to the university for my tuition.

My parents' identity theft left my parents weary of who to trust, so they started to be distrustful of friends and family members, to the point where these relationships became nonexistent. A point came where they were distrustful of each other; particularly with financial matters as the identity thieves used their identities primarily for financial gain. The identity theft ultimately put their marriage in jeopardy.

As previously mentioned, I learned I was an adult/child identity theft victim when I was 19 years old. The revelation of my victim status came when I applied for electric service at my first apartment. The electric company was willing to give me service, but they sent me a letter indicating that they needed a $100 deposit from me due to my credit rating. At the time, I thought it was because I didn't have enough credit established and didn't give it much thought. There was a number at the bottom of the letter they sent to call for a free copy of my credit report, which I did out of curiosity, not out of concern I was an identity theft victim.

Several weeks later, a package arrived in the mail from the credit bureau. Before I opened it, I thought to myself, "They must give you a lot of instructions on how to read these" as I was

expecting something that was, at best, a page long. After opening the package, I was sickened to see that my credit report was 10 pages long and full of fraudulent entries and collection agency entries associated with original fraudulent entries. Whoever had stolen my parents' identity had surely stolen mine as well.

I filed a report with the state police who did not seem optimistic that there was anything they could do to catch whoever had stolen my identity. I started contacting the creditors and collection agencies that were listed on my credit report, armed with the police report, to clear my identity. I was shocked at the lack of support and understanding I received—one customer service representative at a major credit card company told me I was lying about being an identity theft victim to avoid paying the bill!

Over a period of roughly six years, I spent many evenings in tears, thinking I would never have what other people "have"—a decent car, a house—because of the identity theft. I often wondered what I did to deserve this. Who was so angry at me and my parents that they would destroy us in this way?

It was a struggle to establish myself financially as an adult. The first credit card I obtained came with an interest rate of 29%. The financing for the first car I purchased included an interest rate of 18%.[6] The majority of young adults who enter the credit market usually enter successfully with the help of a co-signer. This was not an option for me because my parents' credit was worse than mine due to their own identity theft situation.

It's been nearly 20 years since identity theft began to shape my development and, ultimately, my career path as a college professor. After nearly 20 years, I still refer to myself as a victim as I still receive collection calls and letters over fraudulent accounts that were taken out in my name years ago. I've received court summons over accounts in default that the identity thief established in my name. I ultimately still consider myself a victim because whoever did this to me and my parents is still out there; they still have my personal information and could re-victimize me at any time.

Given my research background and experiences as a victim of adult/child identity theft, legislative support needs to be provided for the following:

(1) Increased collaboration between institutions and agencies that are in a position to support adult/child identity theft victims' recovery. These institutions include, but are not limited to, financial institutions, law enforcement agencies, insurance companies, and credit reporting agencies.
(2) Increased development of effective, targeted consumer education programs focused on adult/child identity theft. Developed programs should target parents and guardians,

[6] Romero, R. (2011, August 31). Children are the latest targets of identity-theft crooks. Retrieved September 14, 2011, from http://abclocal.go.com/kabc/story?section=news/consumer&id=8337313

secondary education, higher education, and agency and organization personnel that maybe in a position to assist adult/child victims.

(3) Increased financial support for the development of victims' services programs for adult/child identity theft victims.

ID Theft Info Source

U.S. House of Representatives Committee on Ways and Means

Subcommittee on Social Security Numbers

Field Hearing on "Social Security Numbers and Child Identity Theft"

September 12, 2011

Written Testimony of the *ID Theft Info Source*™
Linda Foley, Sr. Partner
Jay Foley, Sr. Partner

Chairman Johnson and Members of the Committee:

Thank you for the opportunity to provide written testimony to your committee. We appreciate your interest in the topic of child identity theft and causal factors due to the overexposure and excessive usage of their Social Security numbers (SSN).

In 1999, we founded the Identity Theft Resource Center, a nonprofit victim assistance center, in order to respond to the growing population of identity theft victims who were at a loss as to how to respond to this crime, and clear their good names. Linda Foley had become a victim herself in 1997 and while networking with other victims realized the need for a trained call center, and an extensive website containing documents that both educated people about identity theft and provided tools for remediation. It was while working with both parents of child victims and adults who had been victims of identity theft when they were children that we realized child identity theft needed to be addressed with policy changes and legislation. Both Linda and Jay are considered nationally respected subject matter experts in identity theft and child identity theft. Both of the Foleys were panel members at the DOJ/FTC open forum on child identity theft in Washington DC in July 2011. We have recently started a new company, *ID Theft Info Source*, a consulting firm that will address emerging trends and the issues of identity theft.

For the past twelve years, we have been studying the problem of child identity theft. In the beginning, the perpetrator in the majority of cases was a parent, a step parent, or guardian. Because of this most of the proactive approaches would not have been appropriate because the imposter did not want their fraudulent activities stopped. However, in the past couple of years we have seen more data mining by cyber criminals who then sell child Social Security numbers in underground black markets and on street corners. This change in the pattern of obtaining and using the Social Security numbers of children means we must find a new approach to protecting both the children of today and tomorrow.

Unfortunately, there is not just one solution for this type of crime. While parents may wish to put a freeze or a fraud alert on the child's credit report this would only solve part of the problem. It does not solve the problem of someone using their child's Social Security number for employment, tenancy, college loans, medical care, receive local or federal benefits, and /or tax refunds. In fact, it really doesn't solve financial identity theft issues at all. A credit report begins with the first application for credit. Since a minor may not apply for credit, which is a contractual agreement, there should be no record on which to place an alert or to freeze.

During your hearing you heard from victims of child identity theft and those who represented children who were victims of this crime. No doubt you discovered that these cases became apparent when the child reached 18 and was not able to apply for credit, college loans, or even get a job. You probably also heard from parents who discovered the crime when they were applying for local or federal benefits, or received a notice from the IRS stating their five-year-old had already received a tax refund so therefore their tax return was considered in error.
In our many years of working child identity theft cases we have run across a three month old who owed money to a hospital for work related back injury and a prescription of oxycodone, a five-year-old who owed arrears for child support to himself, and children who have criminal warrants for their arrest that actually belonged to adults who were using the children's information.

Another problem area is **foster children**. Because their Social Security numbers are widely exchanged among caseworkers and guardians, many of these children are victims of identity theft before they even leave the system. And because they have aged out of the system, there are no adults or programs to guide them as a parent might for their own child.

Additionally, when a child becomes a victim of identity theft due to the actions of one or both parents, that child is rarely removed from the home. The typical sentence for identity theft, including child identity theft, is probation. Child Protective Services does not normally follow up on these cases to verify that the parents are not re-offending. Foster children and children of cases where the parent was the perpetrator need to be addressed by legislation to afford them **"special protections under the law."**

Before addressing options to prevent these crimes and assist law enforcement, we would also like to bring to lesser-known problems of child identity theft to the committee's attention.
First would be the **fiscal impact of child identity theft to our economy** and to the individuals affected by this crime. Normally when one turns 18 they are able to pursue further education whether in college or at a vocational school. This enables them to become a productive member of society. Instead, a victim of child identity theft is frequently unable to get the loan necessary to learn a skill or get a college degree. This means they are forced to accept low income jobs.

> *We worked with one young woman whose foster mother left a note for her instead of a birthday card. The note said," the rent is paid until next week." Unable to find any other work she became a stripper in the club living on her tips. That job lead to her working on the streets until she was arrested by law enforcement. The officer who arrested her was familiar with our work and referred her to us for assistance. Upon checking her credit reports we found a five year history of unpaid debts, dating back to when she was*

13 years old. After clearing the fraudulent records she was able to attend a community college while working. Today she is a college graduate and teacher.

Instead of costing taxpayers potentially hundreds of thousands of dollars to prosecute her and prison costs she is a productive member of society. Multiply this times 50,000 and you start to get an idea of the cost to our nation of child identity theft.

The second problem is the **emotional impact of child identity theft**. If the perpetrator is a family member all too frequently the victim is placed into an impossible position of having to choose between watching out for their own self good and perhaps sending a parent to jail, or ignoring the situation with the knowledge that this will impact their ability to get credit for the next seven years. If the perpetrator is unknown to the victim, there is always the question of whether the steps taken to remediate the situation are enough or this crime will be committed over and over again by possibly multiple perpetrators.

The Role of Social Security numbers in Child Identity Theft Crimes:

It is our professional opinion that Social Security numbers in general are overused, overexposed, and abused. We need to re-examine and minimize legitimate reasons for the use of the Social Security number, both for adults and children. Unfortunately, because a person's Social Security number is unique it's not uncommon for multiple governmental agencies, businesses, and other organizations to want to use this as an identification tool.

Your committee has heard from multiple law enforcement agencies including those that deal with cyber crime. It is unnecessary to repeat that testimony. Social Security numbers are so widely distributed that it is nearly impossible to protect these numbers from fraudulent use, especially when talking about the crime of child identity theft.

So what are the options?

It is our studied opinion that we need a two-fold approach in stopping child identity theft and to assist law enforcement in identifying and minimizing these crimes.

1. When considering a long-term solution it is clear that an alternate number needs to be developed for use by minors as a unique identifier. We believe that a task-force needs to be formed to discuss alternate identification tools that could be used instead of the Social Security number until children reach their maturity. This number could be an alphanumeric identifier which would be replaced by a Social Security number when the individual begins to work. This task force should include members of the Social Security Administration, the IRS, consumer advocates, subject matter experts, the Federal Trade Commission, the Treasury Department, Homeland Security, and the U.S. Attorney General's office on legislative issues, to create the necessary pipelines with involved parties, so a more immediate solution could be implemented.
2. *Shiloh's Act;* the 17-10 minor's database: Currently credit issuers are unable to determine the age of an applicant simply by Social Security number. Since people are able to apply for credit by the Internet, telephone, or by mail, not all credit issuers physically see the applicant. When they check with the credit reporting agencies, credit issuers are simply told there are no negative reports associated with that Social Security number. Remember that the first application for credit sets all of the standards of information that will be included in a credit report. That means a credit report could be

created using a child's Social Security number, with a different name and date of birth. There are no other records that the CRA's can use for comparison.

The 17-10 minor's database is similar to the national death registry. It would require the Social Security administration to create a database with the following three fields: SSN, name of person, month/year of birth. When a minor is first issued a SSN, his or her information would be added to the database. When a minor reaches the age of 17 years-10 months old, his or her information would be deleted from the database. The database would be made available via the Federal Trade Commission to the CRA's, DMV's, and other companies or governmental agencies that may need access to this list. Years ago, when we first came up with this concept, the SSA said it might be a workable solution.

When a credit issuer contacts the CRA's to check the credit worthiness of the applicant, if there is no report for that Social Security number the CRA will then refer to the 17-10 minors database. If that Social Security number is on the list the only words the CRA's may tell a credit issuer are: that Social Security number belongs to a minor. It is then up to the credit issuer to extend credit or not understanding that contract may not be binding.

We realize this is not the final solution. However, it should stop the majority of financial child identity theft cases until such time a more comprehensive solution is proposed by the task-force and accepted as policy. The 17-10 minors database will help with the problem of over exposure of the Social Security number in regards to foster children, will help prevent parents from using their own children's SSN when they can no longer get credit themselves, and should assist law enforcement in controlling data mining by cyber criminals of the SSN to either sell or use themselves for fraudulent financial purposes.

We have confirmed that the privacy act of 1974 limits the use of the SSN as an identifier to enroll in the public school so that should not be an issue. Since the majority of health providers no longer use the Social Security number as a medical record number or insurance number and also should not be an issue.

What is an issue is that hundreds of thousands of children every year are having their futures stolen from them due to child identity theft. That is an issue we cannot and should not ignore or put aside as unimportant any longer. If we, as a society and as a nation, do not protect children from identity theft then who will?

Thank you very much for your time and attention. We both offer our time and expertise to serve on the taskforce if one is established or just to be available to the committee as needed.

Linda Foley

Jay Foley

ID Theft Info Source™

Sept. 2011 House Subcommittee Hearing on SSN and Child Identity Theft
Written Testimony by Linda and Jay Foley, 6 pages

PO Box 26502, San Diego CA 92196
Email: **lfoley@IDTheftInfoSource.com**
858-693-7273
Bios:

Linda Foley: An identity theft survivor herself, Linda has spent the last 14 years studying the crime of identity theft. In 1999 she founded the Identity Theft Resource Center and began to work with victims trying to clear their names and restore their lives. In the early 2000's she began to receive more and more calls from parents whose minor children had become victims of identity theft and by young adults who discovered their identities had been stolen before they turned 18. Some perpetrators were family members, often parents, and others were unknown criminals. Linda has spent the last 10 years researching this particular crime as well as other identity theft crimes. She is nationally respected for the depth of her knowledge of identity crimes and has received numerous awards and commendations for her work.

Jay Foley: After his wife became a victim of identity theft, he helped her to found the Identity Theft Resource Center in 1999. Jay's computer and investigative talents lead him to specialize in cybercrime and criminal identity theft. However, he also shared his wife's passion about all types of all types of identity theft. In partnership with Linda, they have undertaken the fight to bring child identity theft to the forefront – believing that even one case of child identity theft is one too many. He has also been working with the California Office of Privacy Protection regarding identity theft and foster children. Jay is also nationally respected for all of work in the field of identity theft and cybercrime. Along with his wife, they have recently founded a new company that will focus on the major issues of this evolving crime.

The Foleys: Together they have been interviewed by hundreds of print, radio, and television media about various topics regarding identity theft. In 2004, they received the 2004 National Crime Victim's Assistance Award presented by the US Attorney General. They have also received numerous commendations and awards for their work in the field of identity theft, victim's rights, and had served on taskforces ranging from the California Department of motor vehicles to the US attorney generals task force on identity theft. In 2010, they were honored to accept the Congressional victims rights Caucus Suzanne McDaniel public awareness award on behalf of of the identity theft resource center and the Foley's work in helping the public understand the issues of identity theft. The Foley's have served as subject matter experts for various state and federal legislative committees and testified in hearings across the country.

James Tielebein

U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Social Security
Field Hearing on Social Security Numbers and Child Identity Theft
Statement for the Record
James Tielebein
September 15, 2011

Thank you to the Subcommittee Chairman and members for the opportunity to share our family's experience concerning child identity theft by a family member by the means of this submission to the record.

My testimony is from personal experience as our family has dealt with child identity theft from 2007 to present and continues to do so. The role of the social security number in this crime was central. I consider the crime which affected me, our family, and my especially my stepdaughter, Gabriella, to be an emerging variety of identity theft. While this case may be defined as theft or identity theft, what happened to Gabbie is that her identity was used by another person to obtain benefits fraudulently.

Background and experience
I have background useful in my testimony, as I: 1) am a licensed private investigator in Iowa. I have been for six years. 2) am an Associate of the Heartland Chapter of the Association of Certified Fraud Examiners. 3) identity theft assistance training from the United States Department of Justice, Office for Victims of Crime. 4) identity theft training from the Economic Crime Institute, 5) work with intellectually challenged individuals who often rely upon proper administration of custodial accounts. 6) experience as a Sheriff Department employee. 7) managed inmate telephone systems for eight years and provided investigative information to county, state, and federal investigators professionally.

I have reported identity fraud to law enforcement previously. Earlier this year I provided information to the FBI regarding a case involving persons using multiple social security numbers to commit federal tax refund fraud. I provided the information to the FBI. It was my understanding that the FBI had no previous knowledge of these crimes. I provided to the FBI the tax refund Declaration Control Numbers involved as and the addresses used. I consider identity crime offensive: 1) as a serious crime against society 2) as well as a property crime when a fraudulent gain is intended. I see those aspects both in the fraudulent tax refund case, and in the crime committed against Gabriella.

This case of child identity theft by a family member
In our case, an offender opened a Uniform Transfers to Minors Act (UTMA) custodial account in the name of my stepdaughter, Gabriella, naming himself as the Custodian. UTMA accounts when properly titled and funded become the property of the minor under the act. A UTMA account is a fiduciary account in which the Custodian acts as a 'caretaker' of the account and the 'Beneficiary' is the owner of the account. Iowa Code 565B governs use and ownership of these accounts in Iowa. UTMA custodial account funds cannot usually be used to offset bankruptcy or other court obligations. This is because UTMA funds are owned by the Beneficiary. Any use of the funds must be for the benefit of the 'Beneficiary,' under well defined law regarding these accounts. UTMA funds must be reported on student financial aid applications.

The UTMA account was opened within a few months after the offender's own bank account was

seized through a 'levy against funds' in 2006. This bank levy was filed by the state Child Support Recovery Unit in Iowa. The person who used the social security number of Gabriella had been behind by child support in excess of $5,000 when he started banking using her social security number with a bank account titled under her name. His success in concealing his income, and by banking under the name and social security of another person is evidenced by the fact that he is now more than $10,000 behind on child support.

The person opening the UTMA account has 13 years of paralegal experience, has recent training in paralegal skills, and has a Bachelor of Arts degree in Psychology by his own admissions. His particular background infers greater than ordinary legal skills and his intent in creating the custodial account. He has made admissions that he has obtained benefits through the 'Iowa Care' program funded by Medicaid. He has made admissions to our attorney that he does not pay federal or state income tax.

Banking records obtained for the custodial account show that the offender used the account to process more than $33,000 through the account during the first 18 months, and nearly $55,000 in total. At times deposits of up to $9,000 would be made, followed by nearly total withdrawal shortly after. Purchases were made for car licenses, liquor, cigarettes, and payment to the 'Iowa Judicial Branch.' These are not transactions that were for the 'benefit' of an eleven year old child. As the transactions were not for the benefit of Gabbie, the offender used her identity to obtain banking services in her name. The account was used only as a pass-through financial instrument by all appearances. When the account was closed out, only about $50 remained, according to records obtained by subpoena.

The bank was notified of the account and we requested bank records for this account in the name of Gabriella. This request was as a request by Gabriella's parent, and on her behalf. Specific request for these bank records under Gabriella's name citing the identity theft provisions under 609e of the Fair Credit and Reporting Act (FCRA) was made. The bank refused. Eventually the banking records were obtained through court-ordered subpoena. Through these refusals by the bank, it became evident to me that Suspicious Activity Reports and Red Flag Rules were not effective in protecting Gabbie from victimization through identity theft.

Official response to child identity theft at times disheartening

Response from those not performing an actual investigation based on the evidence in our case can be described as disinterest or even "deliberate indifference." In an e-mail, I described to the Attorney General office how UTMA custodial accounts are governed by statute and are under the ownership of the minor, yet are under the fiduciary caretaking of the custodian. The reply from the Attorney General office indicated basic shortcomings in understanding of UTMA custodial account law. The quotes below are taken from the AG Office reply:

" ... I am having difficulties making the connection as to how this constitutes Identity Theft. While ...In other words, I'm having difficulties finding where this individual broke the law, or stole her identity. "

"... If my understanding of your statements is correct, this may be why you've been having difficulties getting the police to investigate. While arguably morally wrong, I'm not sure that the individual in question has broken the law. .. If you do not agree with their decisions and believe there has been an egregious error, there are avenues to file complaints to that effect, which I noted in my prior email. This office; however, does not have the authority to force either entity to do what you would like them to."

Janelle Melohn

Compensation and SAE Administrator

Crime Victim Assistance Division

Iowa Attorney General's Office

321 East 12th Street

Lucas Bldg, Ground Floor

Des Moines, IA 50319

Direct: (515) 242-6110

General Office: (515) 281-5044

jmelohn@ag.state.ia.us

Best practices by some officials were exhibited

On the other hand Leaders in law enforcement and Iowa government who have examined our evidence have encouraged us to press for further investigation. Those individuals include: 1) Iowa Senate Democratic Legislative Aide Cathy Engel, 2) State Senator Jack Hatch, 3)State Senator Swati Dandekar, 4)DCI Agent Gerard S. Meyers, 5) US Attorney's Office Coordinator Wade Kizner, 5) Senator Charles Grassley's office, and 6) retired FBI agent and fraud investigation trainer Alton Sizemore. Unfortunately, if local law enforcement will not ask for assistance, all these other resources cannot help. If police will not fill a crime report, then this fast growing crime will not find an adequate response, either nationally or locally. Neither will resources be allocated for that law enforcement response if reports are not made when credible report of crime is made.

Observations regarding this child identity theft case and other issues

The particulars of this case beyond the basic idea that a child should be protected by her government include:

1) Crimes against children are usually considered an enhancement of the crime.

2) Theft crimes that involve a violation of a position of trust. This is usually considered by law enforcement an enhancement of the crime.

3) The state of Iowa seems to be a party to the offense. The state Iowa Judicial Branch accepted payments from the offender, drawn upon the custodial account.

4) The Iowa governor's office and the Iowa Department of Human Services had been notified of the crime. Iowa DHS receives federal funds.

5) FBI and the US Attorney notified on various dates. No response.

6) Offender concealed income from the reach of child support. Arrears of $11,000. He lost $600 due to a bank levy for child support only a few months before opening the fraudulent Uniform Transfers to Minors Act (UTMA) account. Intent can be inferred.

7) Nonsupport is a felony under Iowa Code 726.5. This Aggravated Identity Theft was thus used to commit or conceal another felony - Nonsupport. This is a consideration for enhancement under 18 USC 1028A (c) (4 and 5.)

8) Deposits of $9,000 and $5,000 to the UTMA account were followed by withdrawals for the entire amount on the same or next day. Suspicious Activity Report events were evidently not triggered.

9) Offender has made admissions of obtaining food stamps and medicaid assistance. Fraudulently obtaining a benefit, per 18 USC 1028A. These programs operate with federal funding. Admissions made to an adverse attorney to the offender.

10) Offender has made admissions of failing to file federal or state income tax. Admissions made to an adverse attorney to the offender. Fraudulently obtaining a benefit, per 18 USC 1028A. Violation of Internal Revenue Service Code section 7209. Violation of Iowa Code 714.10.

11) Denial of federal civil and statutory consumer protections under FDIC Red Flag Rules. FDIC requires financial institutions have "Red Flags Rules to protect people from identity theft, under the Fair and Accurate Credit Transactions Act of 2003.

12) Denial of federal civil and statutory consumer protection through FCRA 609(e) request. A letter received from the attorney for the bank refused a FCRA 609(e) request. In the bank's refusal to provide information to an identity theft victim under FCRA 609(e), the attorney provided conflicting information. The bank attorney, on one hand, claimed that the account was a custodial account. On the other hand, the same letter said that all account transactions belonged only to the offender.

13) If not prosecuted, federal and state officials and law enforcement are permitting any and criminals to use instruments like the Uniform Transfers to Minors Act (UTMA) account to commit fraud. This puts in jeopardy the code itself. This code is a uniform act, adopted by virtually all states. Child support enforcement, bankruptcy courts, liens, and other judgments cannot reach the funds, because they are owned by the child per the plain language of the UTMA law. Iowa's version is Iowa Code 565B.

14) Offender makes admissions on his website that he has legal assistant training. http://imaginationtennis.usptapro.com/default.aspx/MenuItemID/351/MenuGroup/ProHome06.htm

Aggravated Identity Theft is a felony crime. Aggravated Identity Theft is a violation of federal Law. The code is 18 USC 1028A.Simply put, it is a violation to use another person's identification, knowing it belonged to another person, to fraudulently obtain a benefit.

Defining a "fraudulently obtained benefit" is usually by plain language of the law. If an offender used the ID to obtain employment, that enables income. Income is money. Money is valuable. If it is valuable, then there is a benefit. This is how states and feds use this definition

in "Immigration" cases. Shouldn't law enforcement use the same language to protect a kid?

A brief list of our law enforcement contacts and results

2007 Information was discovered that Gabriella had a credit report. Dell Computer checked her creditworthiness in 2007 when she was 11.

2008 Iowa Governor office notified by email and phone calls of suspicions that offender was banking through Gabbie's name. The information provided by the Gov. office to Iowa Department of Human Services.

2008 Iowa Child Support Division will not follow up on info, says so in letter to Gabbie's mom.

2009 Info provided to FBI. FBI advises minimum dollar loss thresholds not met for this crime.

2009 Local US Attorney office, Iowa Northern District notified. Advises minimum dollar loss thresholds not met for this crime.

2009 Buchanan County law enforcement. Presented evidence in meeting with the Sheriff.

2009 Handed detailed, indexed, cataloged case book to Omaha FBI SA Robert Kardell.

2009 Contacted Iowa Legal Aid. Advised us child victim does not qualify for Legal Aid Assistance. Gabbie's mother makes just over the Legal Aid intake screening income level.

2009 US Attorney Southern District notified. Advises minimum dollar loss thresholds not met for this crime.

2010 Cedar Rapids Police Investigator John Mathias returns phone call to family. Does not assist.

2010 Gabbie's mother request bank records under Gabbie's name citing FCRA 609e. Bank refuses.

2010 Bank records subpoena sent. Challenged by offender. Ordered by court. Offender found to have been banking through name of Gabbie in a Uniform Gift to Minors account since 2006. Processed $33,000 through account in first year and a half. About $44,000 total.

2010 Linn County Asst. Co. Attorney Betcher does not return phone call.

2010 Iowa Attorney General Office, victim assistance advises return to Buchanan. Cites Iowa law where crime can be reported to offenders local police or to victim's local police. Offers to explain to Buchanan law enforcement.

2010 Iowa Civil Rights division. Advised office policy does not allow involvement. Apparant lack of protection of Gabbie.

2010 Info provided Mike Ferjak, ICAC Investigator, of Iowa Attorney General office conversation at DMAC Cybercrime Awareness Conference, Ankeny, IA.

2010 Conversation Mary Day, Iowa Senator Chuck Grassley office.

2010 Reported identity crime to Buchanan County Sheriff Dept. Incident number assigned was 10004089. Provided BCSD with sworn statement and evidence.

2010 Contacted Buchanan County Attorney Allan Vander Hart regarding status of case. Vander Hart referred victim to Linn County law enforcement and also said it was a civil matter.

2010 Detailed discussion with Special Agent In Charge Gerard Meyers, Iowa Department of Criminal Investigation, (DCI) Internet Crimes Against Children Task Force. Basis for the forwarded email.

2010 4 page written statement sworn to Buchanan County Sheriff Dept., Independence, IA. Provided total of seventeen new pages added to 5/10/2010 incident report #10004089. This in addition to bank statements for custodial account obtained by subpoena for years 2006 -2010. Informed BCSD that Cedar Rapids Police Dept. had referred us to BCSD on March 2010. Previous incident report showed case as inactive.

2010 Sent email to Agent Meyers, DCI. Follow-up up to hour long meeting with him.

2010 Phone call to U.S. Attorney, Victim Coordinator Shari Konarske.

2010 Offender publishes to internet admissions that he has legal assistant training. We feel it may indicate specific intent of banking under Gabbie's name.

2011 Letter delivered to US Sen. Chuck Grassley, Washington, D.C. 22. Advised follow-up would be through legislative staff Kathy Nuebel - Kovarek.

2011 Email with Cindy Robinson of Office of Inspector General, Legal Aid, D.C. On 5/26/2011, Ms. Robinson says she will follow-up. No follow up as of 7/30/2011.

2011 Advised in e-mail to Iowa Department on Aging, Program Director Linda Hildreth of possible case of custodial account fraud. I had attended seminar on financial exploitation and other abuse organized by Hildreth and presented by Jeff Clark, Linn County Asst. Attorney. Neither official returns the email.

2011 Contacts to Buchanan County, Iowa County Assistant Attorney Karl Moorman. Buchanan County, Iowa County Attorney Shawn Harden.

2011 Contacted Linn County Attorney Jerry Vander Sanden.

2011 Letter from Senator Chuck Grassley. We sign the consent form. Certified mail to US Senator Chuck Grassley.

2011 Referral from Sen. Grassley to US Attorney, Northern District.

2011 Meeting with Law Enforcement Coordinatory Wade Kizer, regarding the crime against Gabbie. Mr. Kizner refers the case to FBI office in Cedar Rapids, Iowa.

2011 Email reply from Janelle Melohn of the Iowa Attorney General Office. Ms. Melohn claims not to see aspects of theft or identity theft in the issue described.

2011 FBI Supervisory Senior Resident Agent Mike Kitsmiller phoned in follow-up.

Communicates that FBI will not follow up with investigation because the amounts involved in the theft of the custodial funds and identity theft are in the $33,000 to $55,000 range. It was communicated that FBI requires higher dollar losses to pursue. Also communicated was that family relationship of offender to victim could cause prosecution problems during trial.

Conclusion:

The solution I propose is: 1) law enforcement use the plain language of the law to prosecute these cases, just as they do with other types of crime, 2) That family relationship is not an exemption to prosecution, as with other offenses, and that 3) That existing laws be applied to criminal offenses.

Thank you again for this opportunity to share our experience with child identity theft with the Committee.