

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE  
WAYS AND MEANS COMMITTEE

SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V)

CHAired BY: REPRESENTATIVE JIM MCCRERY (R-LA)

WITNESSES PANEL I:

CYNTHIA M. FAGNONI, MANAGING DIRECTOR, EDUCATION,  
WORKFORCE, AND INCOME SECURITY, GOVERNMENT ACCOUNTABILITY  
OFFICE; JOEL WINSTON, ASSOCIATE DIRECTOR, DIVISION OF PRIVACY  
AND IDENTITY PROTECTION, BUREAU OF CONSUMER PROTECTION,  
FEDERAL TRADE COMMISSION;

PANEL II: NICOLE ROBINSON, NORTH ATLANTIC COAST VOLUNTEER  
COORDINATOR, IDENTITY THEFT RESEARCH CENTER;

MARY C. MCQUEEN, ON BEHALF OF THE COUNCIL OF STATE COURT  
ADMINISTRATORS;

ERIK STEIN, MEMBER, BITS FRAUD REDUCTION STEERING COMMITTEE;  
STUART K. PRATT, PRESIDENT AND CHIEF EXECUTIVE OFFICER,  
CONSUMER DATA INDUSTRY ASSOCIATION; BRUCE HULME,  
LEGISLATIVE DIRECTOR, NATIONAL COUNCIL OF INVESTIGATIVE AND  
SECURITY SERVICES

LOCATION: B-318 RAYBURN HOUSE OFFICE BUILDING, WASHINGTON,  
D.C.

Federal News Service

March 30, 2006 Thursday

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENT....

Length: 18834 words

## Body

---

REP. JIM McCRERY (R-LA): The subcommittee hearing will come to order. Good afternoon, everybody. Welcome to our fifth in a series of hearings on high risk issues relating to **Social Security** Numbers, our SSNs. Today we'll examine the use of SSNs by government agencies, businesses and others, as well as explore options for improving the confidentiality of SSNs.

For many years this subcommittee has worked to protect SSN privacy. For example, the Committee on Ways and Means approved bills in the 108th and 106th Congresses that were introduced by my predecessor, subcommittee chairman Clay Shaw. Some of the provisions from Mr. Shaw's bill in the 108th Congress have become law, including limits on replacement SSN **cards** and a prohibition on the display of SSNs on driver's licenses. The SSN plays a key role in both our government and in our economy. Because the SSN is a unique number for each person and is widely used, it helps link records at all levels. This in turn facilitates administration of government services and benefits, business transactions and fraud prevention. However, once this essential piece of information is in the hands of identity thieves, it opens a Pandora's box of problems. Stolen SSNs can damage lives and businesses' bottom lines.

Today we will hear about the current patchwork of federal and state laws that provide limited and inconsistent confidentiality protection for SSNs. For example, financial institutions are restricted in their ability to release SSN information but SSNs may appear in any number of publicly available government records such as court records or property ownership records. Computers and the Internet have enabled unprecedented information sharing, and anyone who collects, uses or shares SSN information has a responsibility to protect its confidentiality.

Today we'll hear about some of the voluntary steps the government agencies, businesses and others are taking to protect SSNs from unauthorized disclosure. We also will have the opportunity to explore options for improving SSN protections. I'm trying to make this last until Mr. Reyes gets here -- there he is, come on down.

(Laughter.)

These options involve --

REP. : I would have talked long enough to delay --

REP. McCRERY: These options involve complicated tradeoffs. In some cases federal laws or regulations require the collection of SSNs to achieve certain goals such as efficient and accurate tax administration, child support enforcement, and identification of money launderers and terrorists. As we examine alternatives for improving SSN privacy to help prevent identity theft, we must consider the potential effects on the attainment of those goals. We must also be mindful of the cost that individuals, businesses and government agencies may incur as a result. By carefully examining all options to keep SSNs out of the hands of identity thieves and by listening to as many stakeholders as possible, we seek a balance between protecting SSN privacy and allowing its use for legitimate and necessary purposes.

Mr. Levin.

REP. SANDER M. LEVIN (D-MI): Mr. Chairman, since I basically agree with your opening statement and since both of our colleagues are here I'll simply ask that my opening statement be placed in the record.

REP. McCRERY: Without objection. Thank you, Mr. Levin.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
 COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
 REPRESN....

Our first panel today is composed of two distinguished colleagues, Mr. Dreier and Mr. Reyes, each of whom have expressed an interest in the issues that this subcommittee has been exploring for some time now and they were supposed to be here last time but we had a series of votes, and in an effort to not prolong the necessity for other witnesses to stay, we asked these two colleagues if they could come today and they graciously agreed to do that. So welcome, gentlemen. We are interested in your views on this subject. We would like for you to try to summarize those views in about five minutes.

And we'll start with my colleague from California, Mr. Dreier.

REP. DAVID DREIER (R-CA): Thank you very much, Mr. Chairman. Let me begin by expressing my appreciation to you for the hard work that you do in dealing with this issue of Social Security and the specific issue you're tackling right now.

And to Mr. Levin and Mr. Johnson and Mr. Brady, thank all of you for being here. I know we've completed our votes on the floor but this is a very important issue.

Mr. Reyes and I have come together in a bipartisan way to deal with an issue that is getting a great deal of attention. The issue is immigration reform and border security. I don't know if any of you all recall that we dealt with that back in December and our colleagues in the other body are tackling that question right now as to how they move ahead this week and next on this issue.

Virtually everything that we do focuses on the supply side of the immigration problem. On border security, what is it that we did? Well, we talked about building a 700-mile wall, we talked about dramatically increasing the size of the border patrol -- a lot of things that are designed to stem the flow of people coming into this country illegally. But what is it that we really haven't done? We haven't spent much time and effort looking at why it is that they come to the United States of America.

And that's why Mr. Reyes and I, with the encouragement of T.J. Bonner who's the president of the National Border Patrol Council which is the union of border patrol agents said let's not just look at the supply side, let's focus on the demand side here. So why is it that people come into this country illegally? They come here 98 percent of them for one reason and one reason only -- they are looking for a job. They are looking to feed their families. They're looking for economic opportunity. We all know that. And of the 12 million people who are in this country illegally, we know that nearly all of them are here as productive members of society, working, paying taxes, doing things that need to be done in this country.

But we do know that they're here illegally and there is a strong sense that we need to take action. We need to take action to deal with it. Right now there are 94 different documents including that flimsy little Social Security card that was first put into place in 1935 that has not been updated once since 1935 that are used for a potential employee to go to a potential employer and get a job. Ninety-four different documents, including a school ID card, a library card.

So what Mr. Reyes and I have come together to do is very simply to say why don't we make an attempt to put into place a smart, counterfeit-proof Social Security card with an algorithm strip on the back of it, an algorithm strip which would simply go in and look at the data that is already there. No new data would -- the government would not get its hands on any new data at all. This counterfeit-proof card, and actually I carry a counterfeit-proof -- a counterfeit example of my counterfeit-proof card. This is an old Union 76 credit card and I've just put the Social Security card on the top of it. I used T.J. Bonner's picture since this was his idea. And his photo is here and you have an algorithm strip on the back.

And so someone's going in, Mr. Chairman, to look for a job. The potential employer decides I might want to hire this person. They either swipe this card or call an 800-number. They dial the 800- number and it goes into a data bank which is simply taking the Social Security Number, linking it with the Department of Homeland Security, and the only information that would go out is yay or nay. Is this person a qualified worker or not a qualified worker?

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

We put on the bottom of this that this is not a national ID card. I know that from testimony that you all have had in the past from your last hearing, I understood that real concern is raised that, you know, if it looks like a duck, walks like duck, acts like a duck, talks like a duck it may be a duck. The fact is this is not a national ID card. Why? Because the only utilization that this card will be for, number one, Social Security purposes which are correct, and number two, applying for a new job.

Now, as I look around this room I feel pretty sanguine that everybody here, including Xavier Becerra will be re-elected as they head towards this November election.

REP. : Is that an endorsement?

REP. DREIER: Well, you don't want my endorsement, Xavier. You know, that might jeopardize it if you had my endorsement.

But the fact is only people looking, Mr. Chairman, for a new job would be required to carry this. A senior citizen would never have to have a counterfeit-proof Social Security card. Someone who is a small business man or woman would never have to have a counterfeit-proof Social Security card. But what we've got is we've got a situation where the magnet that draws people across the border is jobs. And if the thumbs down comes from this card from the data bank that is already there, we, in our legislation, increase the penalty dramatically and we increase enforcement dramatically. By 400 percent we increase the penalty from \$10,000 to \$50,000 for hiring. And we have a five-year prison term. And we also increase by 10,000 the number of enforcement agents.

Now, you and I were talking yesterday about this and I know that everyone in this room pays their taxes simply because they're patriotic Americans. But there may be some people out there who realize that the Internal Revenue Service is there is that may be the reason that as April 15th approaches they'll be paying their taxes. I know that none of us are among those.

Similarly, if we were to see four or five high profile arrests due to people who were knowingly hiring those who were here illegally, I am convinced that we would see a great diminution of the number of hirings taking place. So I'm convinced that we have, if not the panacea, we have the ability to look at what deals with 98 percent of the people who come here illegally to help us address this issue.

And so, Mr. Chairman, I think we've got a great opportunity to do something here and I'm pleased that members of the Hispanic Caucus have joined again. It's a very, very bipartisan measure. And it's my hope that as we look at the issue of immigration reform we'll be able to recognize that this is better for the employer, easier for the business man or woman who's looking to hire someone because they don't have to look at 94 different documents and they're free of responsibility once they've gotten a yay or nay on it, and it's going to help us deal with this very serious problem that we have of illegal immigration and finally see the Social Security Administration bring that flimsy little paper to which I was referring into the 21st century. So thank you very much.

REP. McCRERY: Thank you, Mr. Dreier.

Now our colleague from Texas, Mr. Reyes.

REP. SILVESTRE REYES (D-TX): Thank you, Mr. Chairman, Mr. Levin and fellow colleagues. I'm pleased to be here with my good friend and colleague from California.

And I just want to make three points but before I make those points I want to tell you that in 1986 when the Immigration Control and Reform Act was passed, it had a provision for employer sanctions in there. Had Congress provided the resources to INS Border Patrol back then we wouldn't be having the debates that we're having today.

Fast forward to 2006 and the three points that I want to make is that, as my colleague stated, the technology has gotten to the point where we feel very confident that Social Security card with biometrics and algorithm and all the other things that have been mentioned were included, it would be safe to say -- I always hesitate from a law

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENT....

enforcement background that something is counterfeit-proof, but it would be very hard to replicate with the kind of technology that's available today. So you need that card that would in essence relieve any employer from the responsibility of having to look at and file as many as nine and ten documents as the I-9 provision currently requires with a fraud proof Social Security card.

Second point that I want to make is that along with that card you need a system, a system where an employer, once he's presented with that card, can check and verify. Whether it's the individual if there's a question, they can ask somebody to come out and check it out or maybe check it out through the computer. Those systems exist today. They are not cheap but I would say they're a lot cheaper than all of these other proposals that have been -- and not as controversial as the ones that have been proposed in the bill that we passed in December. The wall, taking citizenship, all these things that are very contentious.

Third point I want to make is that adequate resources must be provided along with this. No system is good if you don't provide the resources or checks. You've got to provide the money, you've got to provide the people. Our bill does that.

So those are the three basic points I wanted to make. I have a statement that I would like to include into the record but now, being respectful of your time, I will yield back the balance of my time subject to any questions you might have for me or for my colleague.

REP. McCRERY: Thank you, Mr. Reyes.

Both of your statements will be included in the record, your written statements will be included in the record in their entirety.

Mr. Dreier, you said the employer would either swipe the card or call an 800-number. Explain that? What 800-number would they call?

REP. DREIER: Basically what that would mean is that there would be a data bank, the information again that the government already has, no new information.

Is someone an American citizen, are they here on a H2A visa, which is basically a farm worker visa, some other kind of work permit, and they would simply be told yes or no. This person who is applying for a job to work in your company is in fact a qualified worker.

REP. McCRERY: Yeah, but if you're an employer and you call this 800-number, what do you say?

REP. DREIER: What you do is you provide the information that is there, the Social Security Number, and obviously the goal would be to have a swipe for people so that they would be able to utilize the algorithm strip. But there would be a transition period clearly through which they would go that would, you know, obviously the challenge --

REP. REYES: Mr. Chairman, if I could just add to that if you don't mind. What happens today when you go into a restaurant or you go into a shop and you pay with a credit card, they put it into the system, they swipe it or they insert it in a machine readable system. If there's an issue or a problem that they think it may not be you or some other thing, then the merchant will call an 800-number and they will verify the account and all these other things. That's what we have in mind here.

Remember we're talking about employers. Employers that are already used to by and large, as every American is, in utilizing this kind of a system. It won't be exactly a system like the ATM or the credit card system but it will be similar with the card sufficing as proof that it's the individual, that it was presented to the employer and the employer in fact verified it. Any other questions in there about that, there's an 800-number, they pick up the phone, they call and they talk to either a call center or a DHS system that would answer any questions and, again, would relieve the employer of the liability because they've gone and made a good faith effort.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

REP. McCRERY: Yeah, I was just trying to get to the question of why the need for a tamper-proof card if all you need is the number and you can call an 800-number. It seems to me you'd need the card.

REP. DREIER: Well, I think, as Mr. Reyes said, it really would be designed as a backup to deal with --

REP. McCRERY: With questions.

REP. DREIER: Because the goal is to really utilize this algorithm strip that is there that is -- you know, again, and I think that Silvestre's right on target when he says that the notion of saying that something is 100 percent absolutely counterfeit-proof is a bit of a stretch, but there's been no attempt since 1935 to really move the Social Security card itself into the modern era. And I think that we ought to at least engage in the fight, trying to put into place the most technologically advanced mechanism that we possibly can to deal with this.

REP. McCRERY: Would you put a picture on the --

REP. DREIER: Yes, it has a photograph on it.

REP. McCRERY: A photograph on the card.

REP. DREIER: And when the person becomes of working age -- I know that some people raise this question well, would you put the baby picture on because people get their Social Security card. It's when in their state that they would become of working age that the photo embedded item would be provided on there.

REP. McCRERY: Okay.

Mr. Levin.

REP. LEVIN: I'm tempted to ask you a question but I think it involves larger issues. For example, what would happen to the people of working age, the 12 million who are here now illegally?

REP. DREIER: Well, I mean I'm happy to answer that question. I think that part of the goal here is, since we're focusing on this question, if 98 percent of the people who come here illegally are coming to get a job, and with a tamper-proof, smart, counterfeit-proof, whatever you want to call it Social Security card they can't get a job, my sense is that many of them might choose to return to a country of origin. I'm not saying that absolutely everyone but I am convinced that would go a long way towards dealing with this overall sweeping problem that we're dealing with of our border security and the problem of illegal immigration.

REP. LEVIN: I guess my question does open up a larger issue. So we'll leave it for another day since the Senate is kind of monopolizing discussion at the moment.

REP. DREIER: That's why we should weigh in over here a little bit this week on it.

REP. LEVIN: Thank you.

REP. McCRERY: Well, obviously if went to the guest worker program of some sort then that would facilitate getting something like this --

REP. DREIER: Absolutely.

REP. McCRERY: -- that could be used for --

REP. DREIER: But I will say that, you know, I believe that as we do this it's imperative that we have a responsible non-amnesty granting temporary worker program that does go hand in hand with this so that we can meet the economic demand that exists in this country and then tackle the question that you correctly raise.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

REP. REYES: And I can just -- we come together on offering this as one part of the solution but I do believe that we've got to have comprehensive immigration reform. We've got to have secure borders, we've got to have a guest worker program which this would fit in with, and then you've got to take care of -- as Congressman Levin, got to take care of those people that have been in this country paying their taxes, being part of our community. That's what I think will be a realistic way to implement this.

What this does is it becomes part of the mechanism of making sure that we don't have the magnet -- I can tell you from personal experience, after the Immigration Reform and Control Act of '86 we saw a dramatic downturn in attempted illegal entries for about three years. Some areas of our border -- I was chief in McAllen at the time with Border Patrol. Some areas of our border saw a decline in attempted entries into this country of as much as 80 percent. The reason for that was the publicity that was generated that for the first time there were employer sanctions in place, you would not be able to get a job, so the attraction of undergoing that arduous trip through the border and trying to get a job somewhere in this country was gone. But it wasn't until about three years into the program that people started realizing well, you know, Congress didn't allow -- or didn't allot the personnel to check so my uncle or my cousin or my friend said that if you can make it to Denver you can still get a job. Even though it had the requirements of the I-9, there were no teeth in the law.

So I think that this on its own probably is not the whole solution but it gets us part of the way and then comprehensive immigration reform I think would take us the rest of the way.

REP. DREIER: Mr. Chairman, what this does is again, as we look at this question why is it that people come into this country illegally? They come seeking a job. People use a Social Security card, often a fraudulent one to get a job, and this is the way to end that demand side, the magnet that draws them in by having a structure in place like this. And I agree that overall this is not the panacea but I think that this will go an awful long way towards addressing this issue.

REP. McCRERY: Mr. Johnson.

REP. SAM JOHNSON (R-TX): Thank you, Mr. Chairman.

I'm wondering how easy it is to duplicate a card like that.

REP. DREIER: Well, it's a great question, Sam, and I will tell you that one of the things that we've done is we have said that nothing has been done since 1935. And I believe that with the technological advances that are made, that it would be I hope impossible to duplicate it. There are no guarantees, but we should do every single thing within our power to, after these many decades having done nothing, use the technology we have today to ensure that it is as tamper-proof, as smart, as counterfeit-proof as we possibly can.

REP. JOHNSON: I couldn't agree with you more. What kind of upgrade are you going to have to have to get the -- I mean business offices don't have the ability to scan cards, a lot of them.

REP. DREIER: That's a great question and obviously this is something that would have to be phased in over a period of time. But, at the end of the day, I think that it would be easier on businesses because of the fact that they don't have to look at these 94 different documents. And I'm frankly offended by a lot of this stuff where you'd ask one person whether or not they're an American citizen and not another person based on the way someone might look. I'm very offended by that. I think that the existence of this card will go a long way towards helping that. But obviously we'll have to deal with businesses as they look at the challenge of having the --

REP. JOHNSON: Yeah, there's going to be a cost involved.

REP. DREIER: Right.

REP. JOHNSON: And you're from California and you've got a lot of ag migrant workers out there. How are you going to get them a card?

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENTEN....

REP. DREIER: You know what? The fact --

REP. JOHNSON: Let me rephrase this a little bit. Are we going to -- guys that come across legally for migrant work, are we going to give them some kind of an identification?

REP. DREIER: Well, you see what they would have on this is they would within the database it would be stated that they are here if it's an H2A visa or any kind of work permit, that would mean that they're a qualified worker by virtue of it. If we do end up with some kind of responsible non-amnesty granting temporary worker program, someone who is here under that would be able to have this card for those purposes. But if someone is here illegally and they don't have a card, and they are hired, then that employer would be subjected to, as I said, a 400 percent increase in the fine, five years in prison, and he hire 10,000 enforcement agents to make sure that this is enforced. Which gets back to Silvestre's point which is a very important one, if you look at the IRCA, the Immigration Reform and Control Act 1986, we coupled amnesty with sanctions, and un-enforced sanctions is what ended up once again re-igniting this flow of people illegally.

REP. JOHNSON: Well, that's what I was about to say. If you depend on the employer they're not going to do it.

REP. DREIER: Exactly.

REP. JOHNSON: Thank you, Mr. Chairman.

REP. DREIER: And I will say that I didn't believe that the employer should be turned into a border patrol agent.

REP. JOHNSON: I agree.

REP. DREIER: That's one of the concerns that I have and I know we share that. I voted against the -- I was here in 1986 and voted against the Immigration Reform and Control Act for that reason.

REP. JOHNSON: Thank you.

REP. McCRERY: Thank you, Mr. Johnson.

Mr. Becerra.

REP. XAVIER BECERRA (D-CA): Thank you to the two of you for being here and making your presentation. It's rather interesting we are about to have witnesses who will come and give us testimony on the Social Security card, use of the number and so forth, and we've had over the course of actually the last few years a number of hearings. Last session we passed out without a single no vote legislation by Representative Shaw to actually restrict the use of the Social Security Number. And so it's interesting because your proposal would make it the universal identifier and we're about to hear from witnesses who are going to tell us why there are problems in allowing the number to be more universally available. And so it's a fascinating discussion.

We need to figure out a way to be able to identify folks. Right now the Social Security Administration would tell you, if they were here to testify, that just by having a number we can't tell you or they can't tell us if that individual is a citizen or not. They may or may not be able to tell us whether that person is here legally, but you'd have to do a lot of work before you could get the Social Security Number to become a national identification number.

REP. DREIER: Well, we don't want it to be that though. We don't want it to be a national ID card. In fact, as I said, we actually have on this card that it's not a national ID card and it's used only for Social Security purposes and when applying for a new job.

REP. BECERRA: Okay, so then -- Mr. Chairman, let me ask you this: what are you going to tell all the credit bureaus, the banks, all the folks -- all the industries that currently use the Social Security Number. Hospitals used to use them publicly as the patient identification number. What do you tell all those industries that are telling us



HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

right now you can't do more to restrict our utilization of the number because that has become our universal identifier within our industry?

REP. DREIER: See, that's up to them. What I've said is a national ID card. Getting on board an airplane, utilizing it for a federal purpose which is really what we're in the business of doing. I mean the way some private entity or a state or local entity handles the use of this number and card is their business.

REP. BECERRA: So would you prohibit the use for any other purposes?

REP. DREIER: I'm not saying that it can't be used because I mean I don't want to in any restrict the Social Security Number from being utilized for purposes that we determine are necessary, all I'm saying is that I don't want the use of a smart, counterfeit-proof Social Security card to be misinterpreted as some sort of national identification card, that's all I'm arguing.

REP. BECERRA: And the thing there, David, is that if indeed it is a strong identifier that has good firewalls from abuse, then it's going to become a great identifier for a lot of other folks as well because if it works well for identifying whether or not you're entitled to work in this country, someone's going to say it's probably going to work well to identify whether or not you've got good credit or whether or not we should offer you this mortgage. And so I think we have to be very careful. Unless you prohibit its use for other purposes --

REP. DREIER: You know, I think that's something that we might consider looking at.

REP. REYES: Well, you know -- if I can say something. Currently -- I just became a grandfather for the third time. When your baby is born he or she gets a Social Security card. When you volunteer for the Army or the Navy or the Marine Corps or the Air Force, your Social Security card becomes your identifier. When I was drafted I was given a number, RN18746717 -- you never forget that. But today's service people use that Social Security card for those purposes. So, you know, I don't know that -- and I haven't -- maybe David has given it more thought, but I haven't given it a lot of thought in terms of why you would want to preclude or limit somebody's ability to use the Social Security Number when -- I know when I take --

REP. BECERRA: Silvestre, if you were to stay a little longer, you would hear testimony by someone who actually had her Social Security Number misused for identity purposes.

REP. REYES: But, see, even this system I think -- here's what's important about having the system. I made the three points. The system would tell you if somebody else is using the same number because in today's technology, the availability, if someone presents -- say for instance somebody come up with a system of duplicating --

REP. BECERRA: Yeah, but by then it's too late for the person who had his or her identity stolen.

REP. REYES: Well, but the point is it will raise an alert when that card is presented. I mean it's like -- and I don't know how they work currently on use of credit cards but I know that occasionally when I give a credit card, especially when you travel out of the country, they will ask for identification. My wife will get a call at home and say this purchase was made in London or whatever, we want to make sure that you or your husband are comfortable that one of you is in London. So the technology exists that would be able to tell the system that the Social Security Number that was presented in Peoria, Illinois all of a sudden a week later was presented in Los Angeles and maybe within 72 hours was presented in Miami, so that tells you that number's been compromised somehow and the system alerts DHS and they would check all three people that presented that card.

REP. BECERRA: And which one of the two of you is making all those purchases as well.

REP. REYES: Yes.

REP. BECERRA: Mr. Chairman, thank you.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENT....

REP. McCRERY: Mr. Brady.

REP. KEVIN BRADY (R-TX): Thank you, Mr. Chairman.

And David, and Mr. Reyes, it's good to have you here today.

I think Xavier's comment about Social Security Numbers -- one of the issues we are struggling with is our Social Security Number system already so compromised that we can never really bring integrity to the system. But your point is that if Social Security is going to be a key employer verification in this whole immigration border security debate, make it counterfeit-proof, here's the way to do it. I think in the end the question of whether we will have a counterfeit or attempt to create a counterfeit Social Security document -- it isn't a matter of if we do but when and how we do it, how we structure it. And I know that I supported the House bill on border security that passed late last year, but I know that today if we had to rely on the Social Security system to verify workers in this country, either new or existing, the system would simply crater. It doesn't have the integrity, the resources, the technology to do that.

So I just appreciate you bringing a bipartisan idea to the table and I appreciate you, chairman, letting us hear what some of our members who are giving this issue some thought a chance to talk to us about that. So I don't really have a question. Thanks for giving this the thoughtful approach.

REP. DREIER: Well, let me just thank you very much for that, Kevin, and say that I believe that we are in a position where this can go a long way towards addressing those identity issues which Xavier correctly raised, dealing with the question that Sandy raised as to exactly what happens to the people who are here, and tackles this whole issue of the credibility of Social Security and the utilization of the number itself as we head to the future. I had a conversation yesterday with a number of senators about this. They're in the midst of their debate on this. And I should say that this provision is actually included in one of the Senate bills that has been introduced. John Cornyn and Jon Kyl have introduced legislation that actually includes H.R. 98 as an important component of it.

So it's my hope that we'll be able to see this move as expeditiously as possible through so that we can include this as part of a comprehensive package. And I certainly leave it up to you all to demonstrate for us what the best approach is.

REP. McCRERY: Thank you, Mr. Brady.

Mr. Dreier, Mr. Reyes, thank you very much for showing up today and sharing with us your thoughts.

REP. DREIER: Thank you all very much for having us. Thanks very much.

REP. McCRERY: Our next panel is composed of two witnesses, Ms. Cynthia Fagnoni, managing director of Education, Workforce, and Income Security, United States GAO. And Joel Winston, the associate director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission. Your written testimony will be included in the record in its entirety and we would like for you to try to summarize your written testimony in about five minutes.

Ms. Fagnoni, we will begin with you. Welcome.

MS. CYNTHIA FAGNONI: Thank you. Thank you, Mr. Chairman, Mr. Levin and members of the subcommittee. I'm pleased to be here this afternoon to discuss ways to better protect the Social Security Number.

Although the SSN was originally created as a means of tracking workers' earnings and eligibility for Social Security benefits, today the number is used for many non-Social Security purposes. The wide use of the SSN is significant because once it is obtained fraudulently, it can be used to create false identities for financial misuse, to falsely obtain credit, or to assume another person's identity.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

Today I would like to discuss the use of SSNs by government agencies and certain private sector entities, federal laws that regulate the use and disclosure of SSNs, and gaps that remain in protecting the SSN and what more could be done. My testimony is based on reports GAO has issued over the last several years, many of them completed at the request of this subcommittee.

First let me begin with the widespread use of SSNs by both the public and private sectors. Federal, state and county government agencies rely extensively on the SSN to maintain records with unique identifiers and ensure program integrity. Last year we reported that SSNs are available in a variety of public records held by states, local jurisdictions and courts. Public records are documents routinely made available to the public for inspection such as marriage licenses and property transactions.

We also reported that information resellers, consumer reporting agencies and healthcare organizations use SSNs for a variety of purposes, including verifying a person's identity or matching existing records. Earlier this year we reported that banks, security firms, telecommunications companies and tax preparation companies routinely obtain SSNs from their customers for authentication and verification purposes, and sometimes share SSNs with their contractors for limited purposes such as identification requirements, debt collection and data storage.

Regarding the laws, although federal and state laws have been enacted to restrict the use and disclosure of consumers' personal information, including SSNs, no one law comprehensively regulates the SSN use and protections. Moreover, many of the laws enacted are industry specific and do not apply broadly. Several states have enacted laws to restrict the use and display of SSNs. California, for example, has enacted such a law. Thirteen other states now have passed laws similar to California's. Four states -- California, Georgia, Nevada and New York, require notification of security breaches, another example. As a result of such state restrictions, some companies now notify customers of security breaches regardless of where they happen in the country.

Although Congress and state legislatures have enacted laws that help to restrict SSN display and protect an individual's personal information, we have found gaps in the protection of SSNs. We have reported that government agencies at all levels lack the uniform approach to assuring the security of the SSN. In addition, we found that gaps exist in the federal law and oversight of different industries that share SSNs with their contractors. SSNs also continue to be exposed on government-issued ID cards. And finally, few restrictions are placed on information resellers to obtain and resell SSNs in the course of their business.

GAO has made a number of recommendations and proposed matters for congressional consideration to address these gaps. We propose that Congress pull together a representative group of federal, state and local officials to develop a unified approach to safeguarding SSN use at all levels of government. We also recommended that OMB advise all levels of government of the applicability of the Privacy Act, and develop a government-wide policy to ensure a consistent approach for displaying SSNs on ID cards.

Regarding the private sector, we have recommended that Congress consider possible options for addressing the gaps in the existing federal requirements for safeguarding SSNs shared with contractors. We continue to focus on SSN issues, identify gaps, and will continue to recommend possible solutions where appropriate.

Mr. Chairman, this completes my oral statement. I'd be happy to answer any questions you or other members of the subcommittee may have. Thank you.

REP. McCRERY: Thank you, Ms. Fagnoni.

Mr. Winston.

MR. JOEL WINSTON: Mr. Chairman, Mr. Levin, members of the subcommittee, I am Joel Winston, associate director of the Division of Privacy and Identity Protection at the Federal Trade Commission. I appreciate the opportunity to testify today about the important issue of Social Security Numbers and their relation to identity theft.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

Though the views expressed in the written testimony represent those of the commission, my oral presentation and responses to your questions are my own and do not necessarily represent the opinions of the commission or any individual commissioner.

Now, Americans today are very concerned about protecting their identity, and with good reason. Identity theft is pernicious and persistent problem. When a thief steals your identity, the economic and emotional impact can be severe. American businesses pay a heavy price as well, as much as \$15 billion every year. And every time consumers hear about the latest data breach that threatens to expose their personal information, they lose a little more confidence in our commercial system.

Access to **Social Security** Numbers contributes to the worst form of identity theft, having new accounts opened in your name. The SSN has become an all-purpose identifier because of its convenience, its uniqueness to each individual, and its permanence over time. Many businesses also use the SSN to authenticate that the person presenting it is who he says he is. It is this dual use that makes the SSN so valuable to identity thieves.

At the same time, the **Social Security** Number serves many important functions in our financial system. For example, our credit reporting system hinges on the availability of SSNs to match consumers with their financial information. SSNs also are used to locate lost beneficiaries, collect child support and detect fraud among many other things.

This presents a challenge: how to find the right balance between permitting beneficial use, the disclosure of SSNs, while keeping them out of the hands of criminals. The solution must combine a number of approaches. To begin with, public and private entities should lose less sensitive identifiers whenever possible and they must do a better job of securing consumer data. This is a fundamental legal responsibility. Under the FTC Act, the commission can act against firms that misrepresent their **security** procedures or fail to take reasonable steps to secure sensitive information. The FTC safeguards rule requires financial institutions to implement reasonable safeguards to protect consumer information. And the FTC disposal rule requires businesses that hold certain consumer information to dispose of it in a safe manner.

The commission has acted aggressively to enforce these legal requirements. Our two most recent cases involved massive data breaches that led to numerous instances of identity fraud. In both cases the commission alleged that the company failed to have reasonable procedures to safeguard consumer information, including in one of the cases, **Social Security** Numbers.

In addition to law enforcement, education and outreach are critical weapons in this fight. The commission has targeted its efforts at the three groups best situated to combat identity theft: consumers, industry, and law enforcement. We receive between 15- 20,000 contacts per week from individuals seeking advice on avoiding identity theft or coping with the consequences. We provide information and assistance including tools to simplify the recovery process.

We are working to implement the provisions of the FACT Act, many of which address identity theft. The free annual credit report program, for example, has allowed millions of consumers to obtain and check their credit reports where the first signs of identity fraud often appear.

The commission also works with the business community to promote a culture of **security**. Our outreach efforts encourage and help businesses to maintain only the information that they need and to protect the information that they maintain.

Finally, the commission assists criminal law enforcement through our operation of the ID Theft Data Clearing House, a national database with over one million identity theft complaints. Law enforcers ranging from the FBI to local sheriffs use the clearing house to aid in their investigation.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENTEN....

In closing, I want to emphasize that identity theft is a multi-faceted problem for which there is no simple solution. The challenge of determining how best to keep Social Security Numbers out of the hands of wrongdoers illustrates how difficult this problem is. Still, there is much that we can do to discourage unnecessary use of SSNs -- enhanced data protection, educate consumers, and assist criminal prosecutors. The commission will continue to play a central role in the fight against identity theft and we look forward to working with Congress in this endeavor.

Thank you again for the opportunity to testify today and I'd be happy to answer any questions.

REP. McCRERY: Thank you, Mr. Winston. Can you fill us in on what your agency does specifically to try to ensure compliance with the laws that you talked about in your testimony that fall in your jurisdiction?

MR. WINSTON: Well, we go about it many ways. First and foremost we're a law enforcement agency and we investigate and take action against companies that violate the laws that we enforce. For example, cases against companies that fail to safeguard information that they have. We've brought 12 cases to date. We have a number of others under investigation. I think we've sent a pretty clear message to the business community that this is an important requirement.

At the same time we are strong believers in education, both for business and consumers. That's always the first line of defense and we work very hard in that regard.

REP. McCRERY: Ms. Fagnoni, you talked about the fact that many states have enacted laws that restrict the use of SSNs. Can you give us an idea of how those actions by states affect businesses and commerce in those states and maybe even how it affects business and commerce across the country?

MS. FAGNONI: The work we did -- I think we had more information about the impacts on different government activities and the ease of getting information. But one example of how business and commerce has been affected by these laws is that as -- particularly when a state like California, a large state like California enacts a law, for example, the law where any entity where there's a security breach involving information, private information, personal information from somebody who resides in the state of California, the California law is that those individuals have to be notified. Some large companies now have, on that basis, made it a practice to notify anyone when there's a security breach, regardless of what state they happen to live in based on I think kind of the pressure and the precedent of having certain laws in place.

So that's one example where companies have had to adapt and adjust to some of those laws. Having different laws in different states probably can also cause some challenges for people who do business in multiple jurisdictions.

But, as I said, a lot of what our studies have shown is that once -- whether it's government or private entities become more aware of the ways in which the SSN can be fraudulently used and they start to take actions on their own to better secure the information, they can still continue to use the Social Security Number for the purposes that are very important to commerce, but have a better sense and a clear understanding of the need to protect the exposure of that number beyond the uses for which it's needed.

REP. McCRERY: Thank you. Would you talk a little bit about the Internet and the availability of Social Security Numbers on the Internet? Should we be looking at some new federal laws regarding public display of Social Security Numbers?

MS. FAGNONI: In the work we did looking at government and selected private sector use of Social Security Numbers, we did not find a large percentage of entities that were placing the SSNs on the Internet, particular in the local and state government levels. Most of the information that's publicly available through those entities is on paper or microfiche or microfilm and people have to actually go to a location such as a courthouse or some place like that and actually look for the information.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

We do have some work ongoing right now where we're looking at the information resellers who are selling information via the Internet and will have some information to report fairly soon on that. It does raise some questions about how carefully some information sellers are kind of paying attention to who's actually asking for the information and what kinds of safeguards are in place to ensure that the information is being provided only to those where it's an appropriate use.

REP. McCRERY: Thank you.

Mr. Becerra.

REP. BECERRA: Thank you, Mr. Chairman.

And thank you to the two of you for your testimony. Let me ask a question and revert back to the testimony of our two colleagues who were just here and talked about using the Social Security Number for purposes of trying to determine one's eligibility to work in this country. Any comments on what you heard in the discussion that took place among the members on that particular proposal?

MS. FAGNONI: We don't really have work that comment on it directly but there is a difference -- first of all they were talking about having a card that was tamper-proof and there are all sorts of issues associated with kind of looking at the different options and what would be appropriate and what the cost would be. There also is an issue which somebody raised about the information on the card is only going to be as good as the information in the databases at Department of Homeland Security and SSA and we have reported on the fact that, to the extent that, for example, information about somebody's visa status, if that's not kept up to date and isn't updated somehow through the encryption then that's going to limit the usefulness of that.

There's a separate -- and I mean there's a whole separate issue on the deterrent effect which I really can't comment on.

MR. WINSTON: I found the discussion very interesting and I thought the point that you made actually was the one that I was thinking of as well, and that is you can have a national number for immigrants or even for a citizen, but any time you have a number that is the key to benefits, it's going to potentially be something that's valuable to identity thieves. The trick is to find a way of identifying people and authenticating who they are without having that information get in the hands of the wrongdoers and that's a very difficult task.

REP. BECERRA: Now, as we explore how we can better protect the Social Security Number, is there something that we've learned in these examinations about best practices or what some either public or private sector agencies, enterprises are doing to try to protect the number? Anything that you can tell us that can help us with regard to this ongoing examination?

MS. FAGNONI: Well, keying off Mr. Winston's testimony, the work we did where we looked at four sectors -- banking, financial institutions, telecommunications and tax preparers, it was clear that because of the laws and the regulatory structure surrounding the banking and financial institutions industries, there's a lot more -- there are a lot more protections in place regarding the protection of personal information including the Social Security Number. Particularly in telecommunications there really are no laws that are designed to explicitly ensure that telecommunications companies are protecting SSNs. These companies are relying individual contracts and things like that.

So we made a recommendation, actually a matter for the Congress, that one option would be to look at industries such as the banks, the regulatory structures in terms of protecting information and consider whether or not those could be more broadly applied, or conversely to look at some other specific sectors that don't now have laws in place that might warrant them.

REP. BECERRA: Let me ask just one last question and if you wish to comment on something else, that's fine, so long as I have time. I'm not sure how to phrase it. Do we need to have one identifier or should we ask all these

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENT....

various industries to have their own identifiers -- the banking industry or financial services, you all keep an identifier that's for your purposes, credit bureaus, those who are checking status of your demographic, your activities, whether purchasing or anything else, you keep your own number. Government, federal, you keep your own number. State, driver's license and all the rest you keep your own number. Should we have one or for purposes of trying to make sure we don't have a number that can be stolen or has that value if it's stolen, should we try to move to something that says you all keep your own numbers and that way no one can steal that much value from an individual when they get that identifier?

MS. FAGNONI: The reason the Social Security Number is so valuable is because often -- and I'm sure you'll hear this from the next panel -- somebody who's trying to check somebody's credit or make sure they're talking -- that the individual they're talking to is the appropriate person and they should be sharing certain information, the only way they can ensure somebody's identity looking across different kinds of pieces of information is through that common identifier, the Social Security Number. At the same time though, we have a lot of examples where more and more kinds of entities are moving away from particularly the display of the Social Security Number. I think there's a difference between needing it and protecting it because it's a very important way to protect against fraud and things like that.

At the same time, whether it's a driver's license or a healthcare card or whatever, I mean I've seen over the past several years cards that just routinely use Social Security Numbers either first voluntarily and then now routinely across the board use other special identifiers unique to that particular entity for display purposes. But they still have that Social Security Number though behind the scenes that they need for data matching and things like that.

MR. WINSTON: I'll just add very briefly, I agree with that, and there's a lot we can do to convince people to stop using Social when they don't need to. But at the same time we have to look at the back end, and the back end is somebody appears before you with a Social Security Number and wants to take out a loan. How do you make sure that person is who he says he is. And it's the fact that the Social is being used for that purpose as well as for the identification purpose that creates the problem. It's the key that unlocks the door to identity theft and the more we can go to systems of passwords, PINs and get away from using the Social as the authenticator, the better we'll be.

REP. BECERRA: Thank you.

Thanks very much, Mr. Chair.

REP. McCRERY: Mr. Brady.

REP. BRADY: Thank you, Mr. Chairman.

Couple of questions, three really. First two are fairly direct. Identity theft is such a big issue.

What percentage would you guess of identity thefts start with a stolen Social Security Number?

MR. WINSTON: I can talk about the surveys we've done and that others have done which indicate that about two-thirds of identity theft is what's called account takeover and that's where somebody gets your credit card number or your bank account number and gets into your account. Typically that doesn't require a Social Security Number to do. The other one-third is new account fraud where they actually go out and open a new account in your name. Typically, although not always, typically you need a Social Security Number to do that kind of fraud. So it's about one-third.

REP. BRADY: That leads right into the second question. What's the most common way of obtaining a stolen Social Security Number? Is it a stolen card, is it mail theft, computer hacking, information resellers? What's the most common of those would you guess?

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

MR. WINSTON: It's a little hard to tell from surveys because most people don't know how their identity was stolen in the first place, they just know it happened. They don't know who did it, they don't know how it got done. If you look at just the data for people who do know what happened, you find that most of it is done through lost wallets or friends, relatives who get a hold of your information. But that's not necessarily representative of half or more of the people who don't know. So there are a lot of potential sources, it's really hard to tell what's the biggest.

REP. BRADY: Part of the -- final question. Part of the I think complexity is the issue of information resellers, that even if we're able to sort of contain this issue at the source, as it gets sold that integrity becomes less and loose and things happen. Who is -- I'll ask both of you. Who is responsible for ensuring that information resellers and financial institutions and those two whom they sell Social Security Number are only disclosed according to the law and who monitors it? What kind of resource do we use to tackle that problem?

MS. FAGNONI: Real quickly, initially who has sort of authority if anyone is dependent on what industry is involved and that's where we found, at least of the four industries we looked at, and other examples we have where it varies based on the laws that regulate that particular industry. In some cases information resellers for example consider themselves to be financial institutions and therefore subject to the different kinds of laws regulating that industry. In other cases they don't and it's honestly not clear if there is any regulatory framework.

MR. WINSTON: Just to elaborate on that. Generally speaking resellers get Social Security Numbers from credit bureaus, credit bureaus get it from financial institutions. That's subject to the Gramm-Leach-Bliley Act. And there are restrictions on people who buy information from resellers and how they can use -- how they can get the information and how they can use it. We are responsible for enforcing that law as to the non-bank entities, the banking agencies are responsible for the banks.

REP. BRADY: How much resource do you put toward that?

MR. WINSTON: We have a new division at the FTC, the Division of Privacy and Identity Protection which is devoted solely to issues of identity theft, consumer privacy, ensuring that consumer information is protected. So we have a staff of about 30 people who are looking at these issues and enforcing the law.

REP. BRADY: For your agency can you guess or do you know how many businesses have been investigated -- information resellers for example or businesses using it fraudulently have been investigated and successfully prosecuted?

MR. WINSTON: There have been a number but our most recent case against ChoicePoint is a good example. ChoicePoint is one of the largest data brokers in the country and they didn't have procedures in place to ensure that the people who called them up to buy Social Security Numbers and other information were legitimate, and as a result --

REP. BRADY: And thankfully they got a lot of attention, but are we talking about thousands of businesses across the country are investigated, hundred are investigated, dozens are investigated?

MR. WINSTON: (Laughs) -- keep going.

REP. BRADY: Getting a little smaller, is it?

MR. WINSTON: We're a small agency. I don't know what the number would be. It's certainly not in the hundreds or thousands. That's all that we have the resources to do.

REP. BRADY: Thank you, Mr. Chairman.

And thank you, both panelists.

MS. FAGNONI: Thank you.



HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENTEN....

REP. McCRERY: Thank you, Ms. Fagnoni, thank you, Mr. Winston.

Our next panel is Nicole Robinson, North Atlantic Coast Volunteer Coordinator, Identity Theft Resource Center, San Diego, California. Mary McQueen on behalf of the Council of State Court Administrators, Williamsburg, Virginia. Erik Stein, member of the BITS Fraud Reduction Steering Committee. Stuart Pratt, president and CEO of Consumer Data Industry Association. Bruce Hulme, legislative director, National Council of Investigation and Security Services from New York.

Welcome, everybody. Same rules apply. Your written statements will be included in the record in their entirety but we would ask you to summarize those statements in about five minutes.

And we'll begin, Ms. Robinson, with you. Thank you for coming. You may begin.

MS. NICOLE ROBINSON: Good afternoon, Mr. Chairman, members of the committee. Thank you for the opportunity to testify on behalf of this very important topic. My name is Nicole Robinson and besides being the North Atlantic Coast Coordinator for the Identity Theft Resource Center I am also a victim of identity theft.

And I'm going to start first off to tell you -- trying to be brief about my identity theft case but it first started in 2000 and I was notified by a fraud investigator at Kay Jewelers that someone had used my Social Security Number to open an instant credit account. That first night she bought two watches and a ring totaling \$2,300. The next night she came and tried to max out the account and they were alerted to it because people don't usually do that with jewelry store accounts.

Well, I contacted three credit reporting agencies on that Monday. It was very difficult to get my credit reports because she had used different addresses in Texas and I couldn't get my own credit report. I soon came to find out that she had applied for a personal loan at my mortgage lenders. She was picked up by the Bexar County police getting a personal check in my name. My mortgage lender never contacted me although they knew they held a mortgage for me in Maryland and she was in Texas.

The police let her go that day. She promised that she wouldn't do it again, she cried, she said she didn't know what she was doing was wrong and they let her go home. After that since she knew I had a mortgage she applied for a mortgage several days later. She continued to apply for credit even though she had been picked up by the police. She, in a three-month period, got \$36,000 in goods and services. She had a Geico car insurance policy in my name and Geico would not give me the VIN number off the vehicle so I could track that to the dealership that sold it because they said they had to protect her privacy.

As time went on she was eventually indicted and she pled guilty to two counts of misusing my identifying information. She served no time in jail. She was ordered to pay restitution. I have only seen a small portion of the restitution thus far. As time has gone on, I have borne the burden of her theft of my identity. I continue to get her collection notices at my home in Maryland. As recently as last summer I got a collection notice from a collection agency where Nicole Robinson -- and that's her name, her name is Nicole Robinson as well -- she had gone to a dentist in Texas while she was in police custody and had a tooth extracted. Well, of course she didn't pay for it and so the collection agency started to look for her. Instead of finding her in Texas they sent a collection notice to my home in Maryland. I have continued to get collection notices for bad checks that she's written.

I also get pre-approved credit card offers at my home in her name. And the only reason why I know it's for her because we have a different middle initial and they always come with her middle initial.

As I started to get my credit reports, in 2004 I got a 54-page credit report. It had 170 accounts on it -- 130 of them were in collections. It had 42 different names and 65 different addresses. I was notified by another credit reporting agency that my Social Security Number resided on five different credit reports. Even as recently as this year when a mortgage broker ran my credit report, her bad debt, even a judgment from an apartment complex in Texas is on

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENT....

my credit report. And it's not on the credit report that the credit report agency sends to me, but it is on the credit report that they disclose to the lenders.

And as a result of me being a victim of identity theft, I do speak to consumer groups about protecting your **Social Security** Number. The way my **Social Security** Number was stolen by Nicole Robinson is that she worked for a business called Caremark. And Caremark used to provide mail and pharmaceutical services for a law firm where I used to work. Even though I was no longer an employee of the law firm, she still had access to my information in their databases. I ultimately found out that she used **Social Security** Number of several people named Nicole Robinson and she was able to get cars and jewelry. And when she bought a vacuum cleaner, somebody reported to the police in Texas that she had a warehouse full of stuff that she had stolen.

So I just want to go over briefly some of the recommendations from the Identity Theft Resource Center on securing data. And we realize that businesses do use the **Social Security** Number, it is so much a part of what a lot of businesses do, but we think that businesses should take extra precautions to secure the **Social Security** Number. In my case, Nicole Robinson had access to my **Social Security** Number years after I was a member of the health plan that required me to use my **Social Security** Number as an identifier. She should have never had access to that number because I was no longer a member of that plan. And even if she had access to my records, my **Social Security** Number should have been redacted in whole or part.

We believe that consumer education is key. A lot of people don't see the risk in carrying their **Social Security cards** in their wallets and we believe that when you get your annual statement from the **Social Security** Administration, there should be a consumer alert on there about protecting your **Social Security** Number.

We also believe that businesses should assume responsibility for the protection of your **Social Security** Number. If they require it they should also protect it.

Thank you very much.

REP. McCRERY: Thank you, Ms. Robinson.

Ms. McQueen.

MS. MARY C. McQUEEN: Thank you, Mr. Chairman, Mr. Levin, members of the subcommittee. I'm Mary McQueen. The Conference of State Court Administrators is pleased to present testimony on today's hearing before this important committee.

Before I begin my remarks I would like to provide some background about who that group is and I submit testimony on their behalf. I'm a former member of the Conference of State Court Administrators, having served as the chief administrative officer for the court system in the state of Washington for 25 years and most recently assumed the position as the president for the National Center for State Courts. The national center operates in coordination with the Conference of State Court Administrators and Chief Justices in a similar way that the Federal Judicial Center operates with the federal judiciary.

The Conference of State Court Administrators and the Conference of Chief Justices represent the top judicial officials and chief administrative officers in the 58 states, commonwealth and U.S. territories, and we work very closely together with the chief justices to develop best practices to improve the administration of justice. And you may know that more than 98 percent of all judicial proceedings in the United States are in state courts that consist of over 30,000 judges and over 16,000 courts.

Mr. Chairman, let me begin by informing you that the state courts have taken several important steps to protect individual privacy and we share the committee's concerns. The state courts hope to partner with the chair and the members of this subcommittee in your efforts to increase those privacy steps.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

A question we're always asked is why do state courts need Social Security Numbers? What is the state courts' interest in collecting those numbers? And why do state courts require parties to provide them in litigation? I'd like to just briefly identify five different uses of the Social Security Number in state courts.

The first and obvious one to those of you who are members of the Bar is to ensure that accurate information is placed before a fact finder. We want to assure, especially in family law cases, that we have access to the information that's necessary to determine child support, to distribute property, and to determine paternity.

Secondly, we also need to identify the parties. Courts often use Social Security Numbers to identify criminal defendants that lack fingerprint information. We also use Social Security Numbers to enforce judgments and court orders. Courts often order restitution or the repayment of fines as the legal judgment and Social Security Numbers have become the universal commercial identifier for use and monetary penalties. Litigant Social Security Numbers are also necessary for use in state income tax intercept programs where outstanding monetary judgments are deducted from state income tax returns.

Federal law now requires state courts to place a party's Social Security Number in records relating to divorce and child support decrees, and in October of 1999 that requirement was extended to require Social Security Numbers for all children to whom support is required to be paid.

We also need Social Security Numbers to create jury pools and to pay jurors. It requires us when we issue a check to jurors that that income is reported and we're required to have Social Security Numbers for those individuals.

Finally, we use Social Security Numbers to notify the Social Security Administration of incarcerated and absconded persons. The Social Security Administration cuts off payments to person incarcerated in all federal, state and local prisons or jails who are fugitives from justice and they need to identify those persons. And while traditionally that information comes from correctional agencies, the courts initially provide those agencies with that information.

As previously mentioned, the Welfare Reform Act does require courts to collect Social Security Numbers on court orders granting divorces, providing for child support or determining paternity. And Social Security Numbers can appear in many financial records such as tax returns which are required to be filed in many court proceedings.

We were encouraged by some of the language that accompanied the H.R. 2971 and the report dealing with incidental versus non-incidental appearances of Social Security Numbers on public records and we would encourage that if you move forward we would like to work with you on looking at some of those provisions. And in drafting Social Security legislation, we respectfully request that you ask members of the court community to participate in those discussions.

Finally, in an effort to increase privacy and reduce the possibility of identity theft from court documents, the chief justices and the state court administrators have established a standing committee on court privacy and access to court records. They've adopted national guidelines and model court rules, and we've identified three best practices.

I would draw your attention to our visual aid here. These best practices include creating basically two sets of records. The state of Washington, the states of Michigan, Vermont and South Dakota have adopted this approach where basically in the types of records that incorporate sensitive information as well as Social Security Number there is a special procedure for sealing this information, placing them in a separate file and when someone comes to the counter and asks to see the court file, those records are removed in the envelope and not provided to the public.

We've also identified a best practices that we give an alert to the filing party and make sure that they know they're responsible for including any Social Security Numbers in the documents that are filed and make sure that on all

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

court model forms, you know, that everybody uses, that there's an alert saying your **Social Security** Number may be available so please consider not including that.

Also as part of the two sets of records, several states have identified confidentiality filing forms where you put that information on one sheet not incorporated into the court document and that one sheet is sealed. And finally, when requiring **Social Security** Numbers, we've recommended that you only use four digits that would appear in the court record.

So, Mr. Chairman, we recognize the threat of identity theft is real. We commit that the state courts want to do our part in eliminating that opportunity. I've presented several reasons why the courts utilize **Social Security** Numbers as well as the solutions that we're working to implement. Thank you for allowing us to participate in this discussion and I'll be happy to answer any questions you may have.

REP. McCRERY: Thank you.

Mr. Stein.

MR. ERIK STEIN: Good afternoon, Chairman McCrery and members of the subcommittee. My name is Erik Stein. I am executive vice president and the director of Fraud Risk Management at Countrywide, America's largest residential mortgage lender and servicer, currently responsible for preventing, detecting, investigating, mitigating and reporting on criminal conduct by, through or within Countrywide Financial Corporation and its member family of companies.

I am pleased to appear before you today on behalf of BITS and the Financial Services Roundtable to discuss the role of **Social Security** Numbers in identity theft and SSN privacy. I have submitted a more detailed written statement for the record but would like to highlight five key points in my oral statement.

First, SSNs have evolved, regardless of original intent, to become the de facto unique identifier that today accompanies most consumers from cradle to grave. SSNs provide the link to associate consumers to their financial accounts, credit reports, public records, a host of other critical relationships. SSNs are essential to financial institutions to meet various statutory obligations such as knowing their customers, report tax related activity, conduct financial crimes investigations, screen prospective employees and more. All of these functions help keep our customers and their financial assets safe and ensure the **security** and reliability of the economy.

Second, SSNs play a pivotal role in the accurate determination of an individual. With millions of citizens in America, the SSN is the single unique identifier common to them all. However, it's important to note that the verification of the **Social Security** Number is not the same as the verification of identity. Verification of identity is accomplished through the use of other government-issued documentation including driver's licenses and passports which financial institutions require to open accounts and make loans. However, financial institutions have not been afforded the tools to ensure the validity of SSNs and these other documents presented for identity verification even though the institutions are required by the USA Patriot Act to know their customers.

That brings me to my third point, which is the proposed consent based SSN verification or CBSV program recently established by the **Social Security** Administration. It is a critical first step in facilitating identity verification. The program allows verification of the SSN along with the corresponding name and date of birth provided by consumers to SSA's database. I and other fraud reduction professionals strongly encourage the subcommittee to actively support the CBSV program and we urge the SSA to remove restrictions on the daily submission volume by participants, work to improve the proposed response times, eliminate the requirements for a standalone consumer authorization allowing the authorization to be incorporated into loan or account documents, and review the cost structure.

These changes would allow participants to consistently use CBSV on every new relationship, reducing fraud, identifying errors and lowering costs.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

Fourth, criminals know the intrinsic value of SSNs in committing identity theft and other crimes. The sad reality is that criminals in search of identities with which to commit identity theft can readily obtain them through many means. For example, all a criminal need do is steal mail in January when millions of 1099s and 1098s are distributed to taxpayers. These forms are required by statute to display the Social Security Number and for mailing purposes must have the recipient's name and address. We recommend that Congress review statutory obligations that require the printing of SSNs on any documents to determine if the risk of compromise exceeds the value derived. And if so, enact changes to remove these obligations.

My final point is that we should be mindful of the unintended consequences that could result from restricting the use of Social Security Numbers among legitimate businesses. Decreasing financial institutions' abilities to use Social Security Numbers could potentially lead to increased fraud, increased lending costs, decreased loan approval rates, and a myriad of other unforeseen results. It's important for Congress, the SSA and other agencies to thoroughly consider the potential consequences and adverse impacts such restrictions could have on commerce.

In closing, it's important to note that through BITS, the financial services industry has been aggressive in efforts to mitigate identity theft, reduce fraud, and strengthen cyber-security by working together to share information, analyze threats, and implement best practices. We need essential tools such as the CBSV program to continue these efforts.

Thank you for the opportunity to testify before you today. I would be happy to answer any questions.

REP. McCRERY: Thank you, Mr. Stein.

Mr. Pratt.

MR. STUART K. PRATT: Mr. Chairman and members of the committee, thank you for this opportunity to appear before you today to discuss the importance of Social Security Numbers, and for the record, my name is Stuart Pratt and I'm president and CEO of the Consumer Data Industry Association.

We applaud this committee for the thoughtful and open dialogue it has sought regarding how SSNs are and to identify risks associated with such use. Before I discuss how our members' systems make use of the Social Security Number, let's just consider how demographics in our society really explain why the SSN is so important.

First, identifiers in everyday life do change and do so more often than we might think. Over 40 million addresses change every year in this country. More than three million last names changed due to marriage and divorce. We use our identifiers inconsistently. We don't do so purposefully, but a simple example is our choice to use a nickname in some transactions but to use our full name in others. Our name is not as unique as we might think. There are millions and millions of Smiths and Joneses in this country, and in fact more than 13 million consumers have only one of 10 very common last names. Another 57 million males have only one of 10 common first names. We provide other examples of how personal information changes in our written testimony and by taking into account all of these facts, it really does become very apparent why the SSN is the key to stabilizing consumers' identifying information in the context of databases. The SSN is truly a unique identifier.

Let's discuss how the use of the SSN works within our members' systems. Our members design products for determinations of a consumer's eligibility for a product or service, to prevent fraud and to aid in the location of consumers for a variety of reasons. These products bring great value to us as consumers every day. Eligibility products such as a credit or employment report, for example, lead to definitive decisions. These reports are regulated under the Fair Credit Reporting Act, the FCRA imposes a duty that consumer reporting agencies employ reasonable procedures to ensure the maximum possible accuracy of the information in the report. And the SSN plays a vital role in helping our members to achieve this maximum possible accuracy standard.

Absent use of the SSN as a key identifier, consumers would be harmed in many ways through the exclusion or inclusion of information.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

Our members also produce products regulated under other laws such as the Gramm-Leach-Bliley Act. Fraud prevention systems for example employ a diversity of strategies. The SSN plays an important role. In 2004 alone businesses conducted more than 2.6 billion searches to check for fraud. The largest users of fraud detection systems are in fact financial services companies, accounting for about 78 percent of the transactions but there were other users -- 5.5 million location services were conducted by child support enforcement agencies, 378 million searches to enforce contracts to pay, tens of millions of searches were used by pension funds, blood donor organizations, and by organizations focused on missing and exploited children. The availability and permitted use of the SSN remains vital across this entire spectrum of consumer data products.

Consumers and media often assume that the SSN is wholly unregulated and of course this is not the case. As we've discussed, laws such as the FCRA and the Gramm-Leach-Bliley Act do regulate our members' products. However we recognize that similar protections don't exist for all, and the SSN is sensitive personal information that must be protected. We believe that a national uniform to establish information safeguards should be enacted so that anyone possessing sensitive personal information such as an SSN in combination with my name and address, that they would be obligated to protect that information.

There are a number of House and Senate committees that are looking at proposals. I think standards like this would cause more American businesses to move to encrypt such information which we think is the right direction. I think other businesses would decide whether or not they really should be gathering it in the first place. We think that is another good result as well. Our members want to protect that information. We think every company and every business in this country that's going to gather that information should do the same.

Public records also contain SSNs and it's encouraging to hear the state court organizations discussing strategies to protect them. We support this effort unequivocally. However, CDIA does believe that disclosure of the SSN to the general public -- while it must be addressed, we also believe that public records must be made available, including SSNs, to those with appropriate needs. Public records play a vital role in our society and they bring value to consumer data industry products and services. Bankruptcy records, for example, and tax liens as well as judgments are used by lenders. Records of eviction are critical to a landlord, and these are just a few examples.

The public sector agencies are taking actions and we are encouraged by the Social Security Administration's efforts to explore the viability of a system by which a party may verify a particular SSN as associated with another, however the system is cumbersome. It does not allow for real-time automated processing of SSN verification and it will render it very ineffective in fact in assisting victims of identity theft. We hope the SSA will move towards a more effective system in the future.

In conclusion, we believe that enacting law that imposes national uniform information security regulations on all who possess the SSN is the right step to take and this is the right year in which to do it. In contrast, laws that overreach and attempt to limit the SSN's use are likely to merely take fraud prevention tools off the table and out of the hands of legitimate businesses and expose -- and ultimately at the expense of consumers. We believe consumers expect us to protect the SSN. We also know consumers expect us to maintain accurate databases.

Thank you, Mr. Chairman.

REP. McCRERY: Thank you, Mr. Pratt.

Mr. Hulme.

MR. BRUCE HULME: Good afternoon, Mr. Chairman and members of the committee. My name is Bruce Hulme, I represent the National Council of Investigation and Security Services. I'm a New York state licensed private investigator, having been so for 42 years. My company is Special Investigations Inc.

As a profession that has been helping victims through the identity theft maze for years, our experience is that such thefts result from purloining of documents, files, charge slips, credit cards, and wallets. And according to the

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
 COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
 REPRESN....

Javelin Strategy and Research survey, 47 percent of such theft is perpetrated by friends, neighbors and employees. But we agree that additional measures can be taken to further reduce incidents of theft. Our concern is that some measures, unless amended, will have unintended consequences that would help create a safe haven for criminals and do substantial damages to the judicial system.

We support congressional efforts to protect data breaches. We favor limiting the use of the **Social Security** Number on government documents, student IDs and health **cards**, and certainly we do not believe that such information should be sold over the Internet to anybody willing to pay a fee. However, we do have strong concerns with some provisions of H.R. 1745 and a Senate measure that would have direct and harmful effects on how our profession conducts lawful investigations by banning the **sale** of **Social Security** Numbers.

The result would be that databases would not have accurate information about individuals and private investigators would be hampered in our efforts to locate individuals and perform many functions essential to the judicial system.

There are 46,000 American men named Bill Jones. Many of them have the same or similar dates of birth. Private investigators, and others of course, need to be able to differentiate between subjects for many purposes including evidence in court proceedings. One critical and effective tool used by private investigators is what is referred to as the credit header, that portion of a credit report that includes location and identifying information but discloses no credit data. That search is by far the most important one used by investigators when locating female witnesses. Women often change their names due to marriage and divorce, and it also helps to locate other individuals, particular transients.

Pending legislation provides exceptions for law enforcement. This creates an obvious issue of due process because prosecutors with the full resources of the state will always have use of this tool while the **accused** would not. Database searches led directly to witnesses who recanted testimony and helped free a man wrongly imprisoned for 20 years. The same situation holds true in civil matters. Privacy legislation restricting the use of **Social Security** Numbers generally provides an exception for insurance companies, thereby creating an imbalance between the insurance, defense and plaintiff's bars.

Investigators do not have access to a central criminal history database as does law enforcement, so it is essential to develop address information when seeking information about prior convictions so that we know what courthouses to go check out. In both civil and criminal trials, attorneys need to know the backgrounds of witnesses. We urge Congress that any restriction on the **sale** of **Social Security** Number information include an exception to enable licensed private investigators and other state regulated persons to conduct lawful investigations, including but not limited to identifying or locating missing or abducted persons, witnesses, criminals and fugitives, parties to litigation, parents delinquent in child support payments, organ and bone marrow donors, pension fund beneficiaries and missing heirs.

Here's four quick examples of how we use **Social Security** Numbers. I was retained by the New York Courts in a guardianship proceeding to recover \$300,000 in assets stolen from a 97-year-old retired Army officer. It as a successful result. The suspect pled guilty, was sentenced three to nine years in state prison and ordered to pay \$360,000 in restitution and we got all the money back.

In San Francisco, a business owner started getting statements in the mail saying he owed tens of thousands of dollars on computers and other equipment he never purchased. Some had hijacked his identity, opened credit **card** and store accounts in his name, set up a similar type web page in his name and his company's name. The police said they'd only take a report, they wouldn't investigate, they passed it off to the Secret Service. His loss was \$80,000. Secret Service said at that point they had a \$100,000 threshold. A private investigator came into the case and with the use of credit header information found that an ex-employee checking things out had been using three names with several different **Social Security** Numbers and birth dates.

One of our association members reported a case that involved a woman who was left a sizeable inheritance by her uncle in the form of a trust.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
 COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
 REPRESN....

The investigator was able to eventually determine that she was recently married and living in Utah somewhere, destitute out of a pickup truck. That had a successful result.

The former president of our council testified just several years ago I think, a similar case, before this committee regarding a custodial parent whose child had been abducted two years prior. The mother spent two years having a runaround with the police and politicians trying to get somebody to do the job. She went to this private investigator, within basically minutes running a credit header he determined enough leads as to where the husband might be, turned the information over to the police. They went there and got him and the child was reunited with his mother.

As detailed in our statement, the Association of Regulators, which regulates our profession, they support granting an exception for our industry in this. And we stand ready to assist the committee in any way we can. Thank you for this opportunity, Mr. Chairman.

REP. McCRERY: Thank you, Mr. Hulme.

Ms. Robinson, I'm curious about one thing that we have discovered. According to the Federal Trade Commission, 61 percent of identity theft victims never contact the police department to report their identity theft. Do you have any idea why that is?

MS. ROBINSON: Well, from my experience in working with victims, victims feel like the police don't care and, like the gentleman just said, the police will only take a report. They won't actively investigate the crime, they won't actively pursue the perpetrator.

REP. McCRERY: Anybody else have a thought on that? Mr. Hulme? MR. HULME: Well, it's multiple jurisdictions that present problems. Law enforcement basically is just now starting to come up to speed. I can tell you from testimony I heard in the first panel that I've probably investigated more ID thefts than two government agencies. I know many of our members certainly have. And I think it's a question of passing the buck. But it's definitely a major problem that has to be addressed.

REP. McCRERY: Thank you.

Mr. Stein, you mentioned how financial institutions use Social Security Numbers as a tool to help verify the identity of your customers. Could you explain how, for example, a bank's customer identification program might work? What information do you request in addition to the SSN?

MR. STEIN: Identity documents are always requested to prove up identity. Social Security Number helps as a determinant of an individual. As my esteemed colleagues have all represented about the Smiths, the Jones et cetera, the Social Security Number serves to identify the specific Jones or Smith that you're dealing with and to be able to tie those relationships, for example, together within a financial institution to ensure that when you pull credit reports to determine credit worthiness for a loan, a mortgage, a credit card, you're actually receiving the information about the specific applicant who has applied to you so that you can make that credit worthiness decision appropriately. So those are a number of ways in which that number is used. It's not used to verify identity per se, it is used to ensure that you are the Smith with whom we are dealing, and then we use your identity documents, typically a driver's license in today's society, and perhaps other pieces of identification, whether it be a passport, credit card, whatever, to confirm your identity.

The Social Security Number itself doesn't confirm your identity. In the absence of a CBSV or its predecessor the Enumeration Verification System, where we have the ability to actually go out to SSA's database and pull back or confirm the Social Security Number, name, date of birth combination that we know in fact that we're dealing with the same person. The evidence of that, the number itself, simply allows us to tie together disparate people using -- or disparate accounts that are using that same number as an identifier.

REP. McCRERY: Let's take Ms. Robinson's case for example. Another Ms. Robinson stole her Social Security Number, got it, started using it and applied for loans evidently and got them. Why couldn't that financial institution



HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESEN....

have just done a couple of extra things which might have raised flags and made them question the person sitting before them? She probably had a driver's license which had her name which was almost the same, and it may have left out her middle initial and that's not unusual, and so the person at the bank or the financial institution would have said okay. But then maybe he should have looked at the address on the driver's license and then surely the financial institution did a credit check. Maybe they should have compared the address on the driver's license to the address on her credit report. And when those are not the same, a flag goes up and you just either ask her there at the desk or call her back and say there's a discrepancy in the address, you know, in your credit report, what's the deal.

MR. STEIN: I have --

REP. McCRERY: Just a couple more -- why shouldn't you do that?

MR. STEIN: I have two answers. The first one is -- again, going back to the CBSV and the ESV system, had that been commercially available so that the financial institution could have verified the consumer's name along with the Social Security Number and along with the date of birth, and assuming that the person who was misrepresenting didn't have all three of those correct and documentation to support all three of those correct, the financial institution could have had an opportunity right there to have caught that. So number one, I promote that the ability to verify that information is a key step in this entire process.

Now, not knowing exactly what the financial institution saw, and so I'm -- you know, you've sort of asked me to second guess what they did or didn't do here, but with respect to the credit report that would be pulled based on the Social Security Number and the name, I think that Mr. Pratt here has indicated that the volume of address changes that happen in a year and the information tends to lag what gets into the credit reports. And so it wouldn't necessarily, in and of itself as the sole trigger, the fact that the address wasn't in that credit report that represented the person in front of them wouldn't necessarily by itself have been a key indicator.

I also think that in a high volume environment as card issuers deal with, it may also be difficult for them to find those really fine nuances between two people of the same name with the same Social Security Number. I will tell you that had they been using a different name with her Social Security Number there would have been a warning that would have appeared on the credit report that would have indicated there's another name in the bureau that's sharing that same Social Security Number. One of the problems is the very close similarity between the two names in this particular instance.

REP. McCRERY: Okay.

Mr. Hulme, you've stated that your organization agrees that additional measures can be taken to reduce identity theft. You've undoubtedly had a lot of experience in dealing with information resellers. Do you have any recommendations as to how they could improve their protection of Social Security Numbers? These resellers.

MR. HULME: First of all, if there was a manner of getting a lot of the resellers -- I'm not referring to the major ones but two levels down or a level down from selling this -- pull this off the Internet and eliminate sales to the general public and you'll eliminate 95 percent of the problems in my opinion.

REP. McCRERY: Say that again?

MR. HULME: I think one will eliminate 95 percent of the problems if sales of personally --

REP. McCRERY: Could you repeat the whole answer? Pull it from the Internet?

MR. HULME: Yeah. Don't allow the sale of the Social Security Number and personally identifiable information to be sold to the general public over the Internet. That would be my -- I think that would be my first strongest suggestion. And I heard one of the speakers earlier today say different studies that maybe showed that -- I can tell you that anecdotal information, and if you talk to most investigators and certainly our association, we think that if

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENT....

you pull down the sale of these items, of personal information direct to the general public over the Internet you'll eliminate an awful lot of identity theft.

REP. McCRERY: Thank you.

Mr. Levin.

REP. LEVIN: One question to sum up. How easy is it to steal identity?

MR. HULME: Well, I'm not a thief but I would say --

(Laughter.)

REP. LEVIN: I know, I said how easy, not how.

MR. HULME: Well, I think in some cases the door is being left open in some situations. I think there is the availability to get this information and it's being displayed often in areas where it shouldn't be displayed. The information obviously has to come off a lot of government documents, more than are necessary. At times the mail that we get sometimes sent to the wrong place. Even when it comes back to the post office, just check with the postal inspectors and you'll find that they're now and then investigating quite a few crimes regarding what has been done with the mail that's been returned.

REP. LEVIN: So you're saying it's easy.

MR. HULME: Yes.

REP. LEVIN: Anybody disagree with that?

MR. PRATT: I don't think we disagree with that. I just want to emphasize though that the point that has already been made but just to drive it home that fraud prevention systems are moving past the simple question of do you have a Social and a name that match up together. We discuss in our testimony different fraud prevention strategies that are being used today and they really do have to do with bringing together disparate sets of information and attempting to foil the dilemma of having information which is far too openly sold out on the Internet for example by, for example, asking additional questions of the consumer that would probably not -- that the ID thief would not necessarily know. So in an online environment it might be to ask consumers additional questions that the thief probably wouldn't even know if he or she had stolen a wallet.

So fraud prevention systems have clearly moved the simple do you have a set of data and have you matched it, yes or no. And we too agree that the Social Security Administration concept of matching information is a good one, but I suspect we'd all agree that it is not the sum total of how you ultimately validate a consumer's identity. You may be able to validate that you have a real Social Security Number but then you're going to raise yellow flags -- what about that address? The Fair Credit Reporting Act, by the way, was amended in 2003 to obligate all lenders to have a system by which they will compare the old address or the address on the application with the address that you find in the credit report. What about fraud alerts? The Fair Credit Reporting Act was amended in 2003 to obligate a lender to pay attention to the fraud alert, to make sure that it was actually processed so that if one was placed on the file that there would be additional contact measures taken to further authenticate the identity of the individual and attempt to foil the criminal from re-opening up new accounts.

So I think those kinds of steps have been taken and that's why the world is a little different than even the last time I appeared before this committee when we talked about Social Security Numbers and the availability of them. And those are good steps along the continuum and the challenge is thieves become more clever and so too do the fraud prevention systems that have to stop them.

REP. LEVIN: Thank you.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

REP. McCRERY: Mr. Johnson.

REP. JOHNSON: Thank you, Mr. Chairman.

Mr. Pratt and Mr. Stein, I guess you all haven't talked about how some companies will use the last four digits and some of them the first five maybe to identify people. Does that have any validity at all?

MR. PRATT: Well, from our perspective, again Congressman, the Fair Credit Reporting Act stipulated that consumers could truncate SSNs when they ordered their credit reports so that they could look at their credit report. So for example some laws attempt to do that. Yes, there can be some strategies where I suppose truncation works. There are risks any time you start to truncate the number. For example, we actually have run data to show that even with the last four digits of a Social Security Number you can match up as many as 90 different Joneses in this country. So you have to be careful. You have to be careful about when and where to employ a truncation strategy. In some kinds of database management systems that's good, in some that might not be so good. I don't know.

MR. STEIN: I think that one of the reasons that we use truncated Social Security Numbers is a layered approach for role based access. So if there's really -- if you segment a need around Social Security within a financial institution, there's three sets of needs: there's those people who don't ever need to see a Social Security Number. You may have employees who by virtue of their job role have no need to ever see a customer's Social Security Number. And by virtue of that role based access, when they pull up information on the customer to respond to a question or whatever, they shouldn't see the customer's Social Security Number at all. There may be others within the organization who have a need to verify that as a component of the identity verification process but they have no need for the full Social Security Number. They don't need to know the whole thing for that consumer.

So a customer service center for example get a phone call from Mr. Jones and one of the ways they may verify Mr. Jones in a remote environment is by having Mr. Jones tell them, or alternatively key into a voice response unit the last four digits of their Social Security Number as a means to uniquely identify that Mr. Jones is the one for whom I'm going to pull their account records. But again they have no need to see the full thing. And then there are other employees within the organization who have clearly a need to work with the entire Social Security Number and that is a much, much smaller population, so we're reducing the risk throughout that whole thing by taking it from the old world of financial institutions where every employee saw every Social Security Number to a very small number who see a full Social Security Number.

REP. JOHNSON: You know, we tried at one time to get the military to change their procedure but you know all of them use the Social Security Number as an ID and it's on their ID card. Not only that but my wife's ID card has both our numbers on it, not just one. Have you got any suggestions about how we can fix that problem because that's an easy theft I think.

MR. PRATT: Congressman, all I can say is that I think the world has changed enough that it's time to ask that question again of the military to see if they're willing to alter that system now.

REP. JOHNSON: (Laughs.) Okay. We can make them do it I guess.

MR. PRATT: It is true that every time a Social Security Number is used on a medical identification card, when it's used on a -- all the different places that it can occur, those are all risks that I think my colleague to the left has expressed are a potential risk.

REP. JOHNSON: Well, I think you know, Mr. Hulme, you're talking about people stealing your identity. I got stopped at the airport because they said I was a terrorist, you know. Sam Johnson, there's a lot of them around -- (laughs.) And they didn't have to have a Social Security Number to verify who I was. They used other means. So I think there is a way to get around that if we really want to. And you all are probably doing as good a job as anybody. You got any suggestions on that?

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENT....

MR. HULME: All I can say is that some people definitely need to have access to that Social Security Number, but along the same line in fairness it doesn't have to be laid out for the world to have.

REP. JOHNSON: Yes, you're right. Thank you.

Thank you, Mr. Chairman.

REP. McCRERY: Mr. Becerra.

REP. BECERRA: Thank you all for your testimony. It's enlightening and also very disturbing.

Ms. Robinson, let me ask you something. Have you cleared up your credit record yet?

MS. ROBINSON: No, sir. As a result of Nicole Robinson using my data, one of the credit reporting agencies is still reporting her bad debt as mine.

REP. BECERRA: Okay, stop.

Mr. Pratt, you represent the credit bureaus. You hear Ms. Robinson saying that she's been going through this for years. Is there any reason why if we contact you pretty soon you can't tell us that the credit bureaus haven't taken care of Ms. Robinson's credit record?

MR. PRATT: None whatsoever.

REP. BECERRA: Okay. So we'll make sure that you get Mr. Pratt's phone number and you will --

MS. ROBINSON: May I also add thought I have been dealing with that particular credit reporting agency for the last four years over the same problem and it prevented me from getting a mortgage last year because they were reporting \$35,000 in bad debt that belonged to her.

REP. BECERRA: Stop. Mr. Pratt said that you won't worry about that.

MS. ROBINSON: Okay.

REP. BECERRA: So we'll be in touch and certainly you'll be in touch with them.

MS. ROBINSON: Yes, I will be in touch -- (laughs.)

REP. BECERRA: Mr. Pratt, thank you for that.

Mr. Stein, let me ask you a question. What does Countrywide do with customers who for whatever reason close their accounts and their relationship with Countrywide, what does Countrywide do with that personal, private data that it has for that individual?

MR. STEIN: There may be continuing obligations we have even after a relationship is closed -- and let me speak more broadly for the financial institution in general because I think it's true across whether it be lenders or financial institutions. There may be continuing obligations we may have with respect to that information that keeps it within the organization. That having been said, again we talked about this role based access and restricting the access to the information to those who have a true need so that you see only that information for which you have a need by virtue of your job.

REP. BECERRA: But I have a mortgage through Countrywide, I pay it off, I no longer owe Countrywide any money. You have my Social Security Number through the fact that I took out a mortgage with you. I no longer have any banking activity with you. You still maintain a file with my Social Security Number?

MR. STEIN: For our retention period, yes.

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESENTEN....

REP. BECERRA: Which is how long?

MR. STEIN: I believe it's probably either five or seven years.

REP. BECERRA: And who has access to that?

MR. STEIN: Again it would depend on the specific job functions within an organization, but it would be those people who have by virtue of their job function a need to access that information. For example, were you --

REP. BECERRA: Well, let me -- because I'm going to run out of time so I don't want to do that, but let me ask you this: would it be feasible economically for an industry to try to do more to shut down access to that personal data sooner than five to seven years or make it much more restricted in terms of access to that information once there's no need to have an ongoing review of that information because the accounts in essence have been closed?

MR. STEIN: And I don't want to imply that once you close your relationship the same people who have had access to that information when your relationship was open necessarily have it when your relationship's closed. But there's some population that does continue to have it because you may call up a year later or two years later and have some question about your closed relationship that someone now needs to have access to.

REP. BECERRA: Well, let me ask you this: if I were to call your toll-free number to check on the status of my mortgage two years after I've already finished and I punch in on the phone my old mortgage account number and I have some questions I need to have answered so I get an actual voice on the phone, would that person be able to pull up information that would include the Social Security Number?

MR. STEIN: The answer is it depends.

REP. BECERRA: Don't go any further because I'll run out of time. If you can guide us on this. I think what we've heard is that we've got to try to limit the access as much as possible but we also have to recognize that a lot of commerce depends on this information. So let us know what you're doing, what are the best practices that you're using to make sure that once you don't need it you're not using it, and once you don't need it others can't access it. It would be helpful to know who's doing a good job of making sure that we are closing the door on that information the quicker we can. Okay, that would be helpful.

Hypothetical here. Social Security says tomorrow we're going to scrap the current Social Security Number and the system that we've used, we're going to reinstate something totally different. Maybe it's with a number but it's different. Everyone in America who has a Social Security Number you will be issued something else, and at the same time we pass a law saying we prohibit the use of this new Social Security identifier for anything other than Social Security. What do your industries, your agencies, what do you do?

MR. STEIN: Beyond panic I guess -- I think there's several parts to that answer. One, clearly biometrics are being used in certain contexts and so yes, there are -- even today -- again, it's very important to distinguish between how the number is used to create an accurate database to say I have data associated with this number and with this name together versus how I'm going to identify you and make sure that you are 100 percent who you say you are. So even today consumers' acceptance of concepts like biometrics is much greater than it was perhaps a decade ago. So I think you'd find -- you'd always find some sort of substitutes effect. I think the question is at what level of disruption in the system overall, you know, between the time that you were to close off the system completely and then try to reinstate something else. There would be, by the way, a legacy effect. All the data that was currently mediated by SSNs would remain. You know, so court records would remain associated with the Social Security Number.

So you're really talking almost generationally anyway, you're talking about very, very long periods of time as you move away. It does get into discussions of cards and whether cards will have algorithms on them and whether cards will store additional information and whether they're used for limited purposes or more extended purposes,

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

and these are very complicated issues. It certainly goes well beyond the pale of our industry or I suspect any of us here at the table.

REP. BECERRA: Well, one way or the other you'll find some type of universal identifier that can help you keep tabs of the population?

MR. STEIN: Well, I would say two things could happen. Number one, you could have less data mediated which means for example consumers today who already are unhappy when we don't have a certain account that they have been paying on time for many, many years that Countrywide wants to use to approve a loan, when it's not in the credit report they're also unhappy with us, just as they're unhappy when there might be data in their credit report that they say is not theirs. So what you do have with the removal of an identifying system or a single unique identifier like the SSN is potentially dis-intermediating and disconnecting data which can be mediated and which can be used for good things, such as me getting the car loan on the weekend or getting the student loan for my kids and so on and so forth.

So there are effects like that that we probably can't entirely predict today. Even the FTC was asked to look at how SSNs interplayed with credit reports, and that was a study that was done during the 2003 FACT Act. And they concluded that really you move away from a binary good or bad proposition and you're on a continuum -- move one direction and maybe there's less SSNs and so maybe certain types of risks are reduced but maybe you've dis-intermediated data. So it was all about do you move towards more inclusivity or do you move towards more exclusion or separation. And that's the kind of database continuum our members tend to operate on. You know, which way do I go.

REP. BECERRA: Thank you.

MR. PRATT: If I may just take one moment. When you talk about things like biometrics and other kinds of identifiers to uniquely identify an individual and you compare it to the Social Security Number issue, the one thing to keep in mind is that the Social Security Number is a national unique identifier. In the absence of having a national registry of fingerprints, retinal scans, facial recognition, hand geometry, whatever you want it to be, there's no way to take those disparate pieces and put them all together in a credit report. In the absence of that it is probably more likely rather than less likely that the Nicole Robinsons of the world get joined with someone who really isn't them. In this case, the person used her Social with her same name. In other circumstances you're going to have people -- a whole bunch of Nicole Robinsons that may get joined together because there's not that unique identifier that puts them together.

REP. BECERRA: Thank you.

Thank you, Mr. Chairman.

REP. McCRERY: Thank you very much, gentlemen, ladies. We appreciate your testimony and your responses to our questions.

And that concludes today's hearing. The subcommittee is adjourned.

## Classification

---

Language: ENGLISH

Document-Type: Washington-Dateline General News

Publication-Type: Transcript

HEARING OF THE SOCIAL SECURITY SUBCOMMITTEE OF THE HOUSE WAYS AND MEANS  
COMMITTEE SUBJECT: SOCIAL SECURITY NUMBER HIGH RISK ISSUES (PART V) CHAIRED BY:  
REPRESN....

**Subject:** US FEDERAL GOVERNMENT (89%); IDENTITY THEFT (89%); PUBLIC RECORDS (77%);  
LEGISLATION (75%); LAW COURTS & TRIBUNALS (73%); CHILD CUSTODY & SUPPORT (73%); TAXES &  
TAXATION (73%); FRAUD & FINANCIAL CRIME (71%); CRIME PREVENTION (66%); MONEY LAUNDERING  
(66%); TERRORISM (65%); DRIVERS LICENSES (54%)

**Organization:** FEDERAL TRADE COMMISSION (84%); US GOVERNMENT ACCOUNTABILITY OFFICE (84%)

**Industry:** IDENTITY **SECURITY** (77%); BANKING & FINANCE (72%); DRIVERS LICENSES (54%)

**Person:** JIM MCCRERY (59%)

**Load-Date:** April 7, 2006

---

End of Document