FEDERAL TRADE COMMISSION

SECURITY IN NUMBERS
SSNS AND ID THEFT

Monday, December 11, 2007

9:00 a.m.

Federal Trade Commission

FTC Conference Center

601 New Jersey Avenue, N.W.

Washington, D.C.

FEDERAL TRADE COMMISSION

I N D E X

PROCEEDINGS

- - - - -

MS. COHEN: Good morning, everyone, and welcome back to the second day of the Security in Numbers Workshop. We're happy to see so many people back for the second day.

We spent yesterday exploring the different ways that the private sector uses the Social Security number and, today, our first panel is going to look at alternatives to SSN restriction for preventing identity theft and then our last panel is where all of you, hopefully, will get involved and we will consider possible recommendations that the President’s Identity Theft Task Force can make on this issue. As I said, this last panel is meant to give all of you an opportunity to ask questions of the panelists, but also to voice your opinions. We hope that everyone gets an opportunity to speak, so please be mindful of time when you're giving your comments so that everyone who wants to voice an opinion is able to.

Just a few housekeeping notes, pretty similar to the ones of yesterday. If you leave the building at any time, keep in mind that you need to go through security to reenter. Please wear your name tags at all times, and if you notice anything suspicious, report it to the security, to the guards in the lobby. Please turn off or set to vibrate your cell phones and don't use your cell phones anywhere in the conference area because it does mess with the webcasting equipment. You can use your cell phones in the lobby or in the phone room that’s next to the registration desk.

The rest rooms are located across the lobby and behind the elevators. Fire exits are through the main doors at the front of the building on New Jersey Avenue and straight back through the pantry will take you to a corridor that will lead to G Street. In the event of emergency, proceed to the building diagonally across Massachusetts Avenue.

The FTC is offering a free WiFi hot spot and brochures are on the materials table that give the key if anyone wants to use that. And, finally, I would like to thank IAPP for the magnificent breakfast spread that I've been enjoying this morning and I hope all of you have.

And, now, without further delay, let me introduce Betsy Broder who is the Assistant Director for the Division of Privacy and Identity Protection at the FTC.

PANEL 5: ALTERNATIVES TO SSN RESTRICTION

MS. BRODER: Thank you, Kristin. Yesterday everyone started off thanking the FTC and we really appreciate that. So, I'm going to do the same.

I want to, once again, recognize the team who have spent the last few months compiling the summary of comments, interviewing dozens of experts, many of them in this room, coordinating this workshop, and ensuring that all viewpoints were considered. Under the leadership of Pavneet Singh, Kristin Cohen, Chris Olsen, Katie Race Brin, Marcy Baskin, Callie Ward from our Office of Consumer and Business Ed have done an exceptional job and I think they deserve tremendous praise. So, I thank you all very much.

(Applause.)

MS. BRODER: Okay, now, let's talk about me. Several years ago, I did a television interview on identity theft and I was asked a question that I simply didn't know the answer to. I responded candidly that I just didn't know. That afternoon, I returned to my office and I got a call from the press office asking -- there was an invitation for me to do a radio interview that evening. So, when the interview began, the host said he knew that he had to have me on the show because he never before had heard a federal official publicly say that they didn't know the answer to a question.

That was a joke.

So, the President's Identity Theft Task Force recognized that it didn't have the answer to the question of how to address private sector uses of Social Security numbers. There was a lot of talk about them being the keys to the kingdom and others argued that more information, not less, was the clear way to reduce identity theft and fraud. This is a complex issue, and I think it's clear from yesterday's session that there is no single silver bullet.

We heard yesterday the various ways that the private sector relies on Social Security numbers to identify, track, match consumer data, as well as how Social Security numbers are used in the authentication process. And today's panel will pick up where we left off yesterday.

So, let's assume, for purposes of this panel, the private sector entities will continue to use and maintain Social Security numbers for the various purposes described yesterday. How, then, can we minimize the value of Social Security numbers for identify thieves? Would more robust authentication practices filter out enough fraud?

Somebody referred to empowering consumers to control access to their information. How effective are these defined limits such as fraud alerts or credit freezes?

Another option raised by Emily Mossburg and Jonathan Cantor yesterday was a federated identity program where a trusted third-party vouches for a consumer's ID. Is that part of the answer? And how do consumers experience these options?

Our panelists will each give a short presentation. I will ask several kickoff questions and then I'm going to open it up to the rest of you. I want to remind all of you, as Kristin said, to keep thinking about possible recommendations. Write them down as we talk and hold on to those thoughts for the last panel.

I now want to briefly introduce the panel of outstanding experts we have this morning and then we'll start hearing from each of them on various perspectives.

To my left, Chip Tsantes is the Chief Technology Officer of Intersections, Incorporated; to his left, Bob Blakley, who we heard from variously during the session yesterday, is the Principal Analyst of the Burton Group; Stuart Pratt, to his left, is the Chief Executive Officer of the Consumer Data Industry Association; and to his left, we have Jeannine Kenney, just in from Washington gridlocked traffic, the Senior Policy Analyst at Consumers Union.

So, Chip, if you could kick things off.

MR. TSANTES: Great, thank you. What I'd like to talk about is all the things we look at besides SSNs as we are authenticating people.

I’m with Intersections, you've probably never heard of it, but Intersections is the largest provider of identity management solutions for consumers. So, you have heard of our partners, Bank of America, Citibank, Discover and other banks. Most of our products are sold through big financial services partners, but we also have other distribution channels. We’re a background screening company. We have other information companies all centered around that kind of information.

So, let me talk about our consumer business and what we look for. So, you come in, you want to get access to your credit information, you want to get access to your public record data. We'll sell you your IDA score, which you heard about yesterday, which is interesting. We'll sell you everything that Sizant, LexisNexis has about you and, also, we’ll send you alerts when any of that information changes.

So, we look at your AVS on your credit card does that match the address you gave us, does that match the address the postal service has on you, does that match the address the credit bureaus have on you? We look at your CVV, do you have control of that credit card? If you came in by phone, we’ll look at caller ID. Did you come in, did you spoof that, does that make sense to us. Same thing with your ISP trail, we'll look at that, where you came in from and does that match the information you're giving us.

We'll get your e-mail address. It turns out when fraudsters come in and then they're trying to come in to get identities on 100 people, they make up e-mail addresses in a pattern. We look for those patterns and those are known to us.

We ask you questions, in and out-of-wallet questions. What's interesting about the out-of-wallet questions are the states are starting to dry up that information. So, a couple of examples yesterday of what color car you had, states aren't reporting that information any more. If you look at Virginia, where I live, it does not report auto information. So, you can't ask me those questions as easily as you once could. So, we're going to have to come up with some better sources of data for some of those out-of-wallet questions.

And then we look at, you know, has anybody at that address opened another account, has anybody with that credit card used another account. It's, obviously, a sign to us if more than a couple of accounts are opened using the same credit card.

So, again, these are obvious things, but we triangulate all of that information to make sure that we're talking to the right person, that we're looking at the right person. If any of those things don't add up, then we turn it over to some investigators who will do some more research, possibly call, and if we're still not sure, if someone tries to come online and wants fulfillment online, we’re not going to give it to them online. We’re going to mail a credential to the address of record and then they can open the account from there.

So, again, we do a lot of things to make sure that even though you have the Social Security number, you don't get the keys to the store for someone's personal identity as we're looking at that information.

Let's talk about the user-defined alerts here for a minute. We, like I said, do a lot of alerts and we're expanding those to people. And it's not just that you need your credit information alert, you need your public record data alerts. I talked to someone last weekend who was a victim of an identity theft incident that's a little different. She was pulled over at a traffic stop. The officer took the license and said, you know, you're coming with me to jail. It turns out someone had used her Social Security number and her name to get a driver's license, had been arrested for drunk driving at a different address, of course, she never knew about it until she was arrested. So, again, those public record data reports and alerts with that kind of information would have alerted her to something that has now taken her over a year to try and clear up and cost a lot of money to make that happen.

The other thing we're doing, which is interesting, is we’re doing Internet surveillance. So, if you register your credit card or your Social Security number with us, we'll look for it ourselves and through our partners to see if we can find it anywhere. Because if we can find it, then that's bad. That probably means a fraudster has it or it's been posted on a bulletin board or some chatroom or something or someone's mad at you and posted it somewhere and we'll also give you the context we found it so you can, you know, better know how that got there so you can prevent that again.

Talk about fraud alerts for a second or people who are sensitive to that, they could be the victim of fraud. We see that in our call center all the time. People call up and say, hey, put this extra credential on my account because I'm a little nervous, I'm a little worried. Typically, that's someone we find who's going through some life crisis, a divorce is typical, they're going through something where they want to better protect their financial assets and the information about their financial assets. Or there's someone maybe in the home with a drug problem or something and they're trying to prevent some other event.

So, people get sensitive to that, and we do support sort of this notion of a temporary fraud alert that can be put on when you know you're in crisis, when you know you're in alert and, in fact, we've automated that through our partner TransUnion today.

Let me just say that authentication is difficult. I'm glad to see so many practitioners here who are in the trenches using authentication. I was at a Commerce Department meeting a few months ago and there were maybe 20 people at the table speaking. It turns out I was the only one who actually had to authenticate people day-to-day for a living. Everyone else was a pontificator. But it’s good to see everybody here.

We're working on a lot of things going into the future and we'll talk about some of these things today, whether it be an authentication utility, which I'm very supportive of if we can find someone who most people can trust. I don't think we'll find someone that everyone can trust. But I'm not sure who that is. I'd like it not to be the government, although I'd like the government to sanction it. But who is that?

Is that Google? Probably not anymore, they've eroded trust in some of the things they’re doing. Is it Microsoft? They’ve not been able to do it. I'm not sure who it is. Maybe it's someone like the Financial Services Roundtable who, with a consortium of banks and most people trust banks because they put money there, can do it. I don't think one bank can pull it off.

At my previous career at Accenture, I did some work with a trading consortium and when one bank tried to do it, no other bank would participate because they think the one bank has the advantage in the solution. When they all participate, then those things seem to work.

Finally, I think in the U.S., I’m hopeful, that your mobile device will become a way to do strong two-factor authentication, something everyone carries now, something everyone knows how to use. You can put technology similar to an RSA token, a strong two-factor token on there that you can unlock with a PIN, again, a secret that only you would know. It can't be transferred to another device, you can lock it to this device, and I think we're going to see some exciting things around the mobile device going forward. Thank you

MS. BRODER: Thank you, Chip. Bob?

MR. BLAKLEY: Thanks very much, and I do very much want to thank the Federal Trade Commission for hosting this workshop. It is really encouraging to see such a not only a civil, but informed discussion on an important topic.

Authentication is and always will be hard and imperfect. So, it should not be surprising that we have a problem with authentication using Social Security numbers.

I also want to commend the Federal Trade Commission for not moving precipitously on this. One of the lessons of the difficulties that we're currently having in Iraq is that if you get rid of a system before you have designed the system that you are going to use to replace it, you can end up with a problem which is worse than the one that you started out trying to solve.

And I think the testimony yesterday adequately demonstrates that there are a lot of uses of Social Security numbers upon which all of us depend, and even though the current solution is imperfect, we could create a lot of damage by doing something that is poorly thought out.

Having said that, I'm going to talk about five things that are poorly thought out in the sense of not being completely proven in the market and suggest that they are things that we ought to, at least, do some more thinking about.

The first is when we speak of authentication, particularly in online security contexts, we typically think in terms of getting additional strength from additional secrecy. This isn't, however, always really the way the world works. In some cases, problems that look like problems of strength are actually problems of symmetry or problems of time. So, it is worth looking at the question whether the fact that the bad guy knows that his victim exists, but the victim doesn't know that the bad guy exists, is an asymmetry that is giving rise to some of our problems and trying to fix that.

One of the things that we could do, for example, is instead of calling the phone number of record or emailing the e-mail address of record, we could, whenever a consequential transaction involving a Social Security number is initiated, maybe notify the last two or three addresses with the theory that if there is a fraudster on the account, at least we might also get the real owner and have a dispute brought forth into the public that would then have to be resolved in some way.

It's also interesting to ask whether, if you asked a fraudster, if you just called up out of the blue and said, you know, I'm looking for the owner of Social

Security number XXXYYZZZZ, he might not involuntarily say no, because he's got 37 numbers that he's got to remember whereas an honest person typically has only one.

Other things that you might want to consider are eliminating or reducing windows of vulnerability. So, if I go to -- so, as Annie Anton said yesterday, it is ludicrous to be pretending that a Social Security number is a secret when using it for authentication in a transactional context. On the other hand, when you use the Social Security number in a vetting context, when someone is establishing a new account, that's a different kind of use and it's very hard to get rid of because you have to use something to link a person to his or her past history. And as we had observed repeatedly from this seat yesterday, the Social Security number is, in a certain sense, the only unique piece of information that links the majority of components of a person's history to them.

So, when you're using a Social Security number in a vetting context, if, for example, the legitimate owner of the Social Security number were to receive a phone call in real time saying, do you think you're opening an account right now and they had to answer yes before you performed the transaction or else you, for example, go to the alternate channel that Chip talked about and mail something to the address of record and proceed from there, that might reduce a lot of fraud.

Incidentally, or perhaps not so incidentally, it is this linking of a person to the details of their history that the Social Security number most importantly does and that's also the reason why it will continue to be vulnerable and why no other artifact can be designed which is not vulnerable.

So, if you look at what happened to some of the residents of Hurricane Katrina, all of the details of their previous history were destroyed in the incident, and those people must have a way to reestablish some sort of identity that allows them to function in society. But there is no remaining history to be linked to there.

So, no identifier is going to be free, completely fraud resistant in that context because there's a bunch of people who simply don't have any records any more and we've got to find a way to give them identities, and this is the problem that we're trying to solve with Social Security numbers when somebody loses a marriage certificate or a title deed or something like that and needs to go to an office and reestablish a connection with the past. That's the opportunity where fraud creeps in and it's not possible to eliminate that, in general.

I'll talk about, I think, three or four more things. The first thing is that we can eliminate some dependence on Social Security numbers in contexts where it's not necessary for us to have all of our identity with us at the same time. So, having your Social Security number and the rest of your identification details all sort of linked in a central file is similar to requiring you to carry the title deed to your house and your entire net worth in a cashier's check around in your wallet all the time and, therefore, subject yourself to complete bankruptcy and destitution if you ever get robbed.

It's not necessary to do this and, in fact, many people don't do it. They create things like limited liability corporations in which they invest portions of their assets and shield the rest of their assets from any sort of damage that might happen.

One of the ideas that we have been discussing on our blog at the Burton Group is this notion of the limited liability persona which is essentially the same construct, but extend it to individuals and with less cost and fuss at time of creation. The reason limited liability corporations have franchise taxes and are otherwise expensive is because we expect people who have them to be making a profit and to be gaining a tax advantage.

If you just want to give an individual a way to create an identity with a tax ID number that could be thrown away if something bad like identity theft happened, and you don't expect them to be earning revenue via this legal instrument, then maybe you could give them a legal instrument like an LLC, but, for this limited purpose, cheaper and then allow them, for example, to get a secured credit card in the name of a limited liability persona in a limited amount, so that they could perform transactions in dangerous environments like the Internet. And if something bad happened, they would be out $3,000, but they wouldn't have to lose their house or their marriage. So, that's one idea we've been talking about.

Another idea we've been talking about is the notion of eliminating externalities. There are currently a lot of externalities in the identification system, and by externalities, I mean possibilities for the creation by one party of a loss which is suffered by another party. The sort of classic behavior with respect to an externality is that the party creating the loss has no incentive to mitigate it because he doesn't suffer the consequences.

It would be possible to continue to allow use of Social Security numbers, but to impose liability for damages consequential to their loss, and it would also be possible, in conjunction with that, to create safe harbors so that organizations which chose to outsource their identification and authentication services to third parties who were recognized by the FTC or another organization as being good at this, could escape at least some of the liability associated with losses due to identity fraud.

The FTC already does this in another area in compliance with child privacy legislation, COPPA legislation, they recognize at least one third-party infomediary, a company called Privo, which authenticates the relationship between a parent and child and then allows the child to create an account at a third-party, but without having to give any personal details to the third-party and, therefore, without subjecting the third party to any COPPA liability. They’re an FTC designated safe harbor for that purpose.

They're an example of something we’ve called on our blog an identity oracle, something which maintains personal information about individuals and which performs an authentication task, but which does not pass on the information it has to the relying parties, the people on whose behalf it's authenticating people. Instead, the organization, the identity oracle, assumes some liability for correctly authenticating people and, therefore, becomes a repository of good practice and also develops a sustainable business.

Finally, I do want to say I think Chip's right, I think some day not too far in the future we will all have something like this. Mine is sitting in my bag there, and I hope it doesn't ring because I didn't get a chance to turn it off before I came up here, but I think we will all have a lifetime portable cell phone number and will be reachable on this channel. And things like I believe it was the OATH technology that you're referring to, Chip, I was the chair of the committee that wrote the OATH specification that allows you to do one-time password identification on a device like this, are possible avenues toward a little bit safer authentication in the future.

Thanks to everybody for coming.

MS. BRODER: Thank you very much and we'll follow up on some of these ideas in our final panel.

Stuart?

MR. PRATT: First of all, let me just -- all right, I better speak in this direction, right, Betsy?

MS. BRODER: Please.

MR. PRATT: My thanks to the FTC for structuring this program. It’s actually really well done, Betsy. I think the FTC did a really great job.

We've explored authentication, we've explored why the SSN is important for linking, data matching. Today, we'll talk a little bit about restrictions or not and what we can do to minimize, I suppose, the net value of an SSN relative to other match points and other processes that are either in our hands today or could be in our hands in the future. Really, this is more or less a dialogue on a continuum as opposed to a perfect point in time where we will know everything that we need to know in order to solve this problem.

But it's a great program, we appreciate the deliberative approach that you've taken to this as well and we're very glad, as the CDIA, to be a part of this discussion now and going forward as well.

So, just a few points, I think, from our perspective. The CDIA represents really the data industry that manages and primarily third-party databases, but our members produce the authentication products that are used in the marketplace today to prevent the types of fraud that we're concerned with. Our members produce the risk management databases that help to mitigate risk and protect consumers and maintain in, for example, the financial services space, safety and soundness of loans.

So, our members are on the front line of producing the products that produce the solutions that result in a far better marketplace here in the United States today. Because when you look at the sheer volume of transactions in the marketplace today relative to the crime that we're discussing here today, there still is quite a success story that's out there and I know, Betsy, we're concerned about overstating trends, but some of the trending is at least positive.

And, Joel, I know you were on a panel recently where I think you and one of my associates had a good discussion of that as well. But there is some positive trending out there. It's not definitive. We're not going to call it definitive. There's probably more work to be done in that area. But from our perspective, to the extent that there's positive trending, it's because we have begun to move up that curve towards the top of the bell curve. We're no longer right there on the left-hand side of it.

So what do I mean by that? Well, a couple of things. First of all, when we talk about identity theft, I think the FTC's done a good job of breaking it out not only into two component parts, but their most recent polling really refined that into a different level of granularity as well. But you really have new account versus current account types of frauds, and the value, the net value of the SSN is different in the new account versus the current account context, for example.

So, for example, I have a hard time believing either Bob or Chip or Jeannine, any of us would say you should use your Social Security number as a PIN number for your current account. I mean, you know, but let me give you an example of the challenge we still have even with -- there's a lot of knowledge in this room, but I had a reason yesterday to order my birth certificate. So, I called my home state and a very nice young lady took down information for me. And then she said, well, Mr. Pratt, I have security questions for you. Then she read to me, is this your address, yes; is this your phone number, yes; is this your Social Security number, yes.

Kind of reversed the whole process, didn't it, right? So, she felt really good about her security protocols, but, of course, she had no clue where that birth certificate was going. But this was a real birth certificate with the embossing on it and the whole bit.

So, if we walk away with nothing else, the truth of it is there's still a lot of training and a lot of knowledge-based work that has to be done before we even get to some of Bob’s futuristic discussions, which are good ones, not long-term futures but maybe near midterm futures. But we're still talking about just training people today to just be smart about authentication right now. That's really at the core of something CDIA is going to push on very hard is being good at managing and securing the data that you have today.

The program has a great question, the program description, Betsy, has a great question, and the question is would essentially authentication, more authentication reduce the value of the SSN, and the answer is yes. In fact, again, some of the trending that's out there, the small percentage of ID theft relative to the large percentage, even if you just take this binary breakout between new account versus current account, new account fraud is -- back in '03, I guess it was more or less 33 percent, and now if you use the new FTC polling data it shifts closer to 20, 25 percent. We’ve seen other data sets that indicate similar differences.

Well, the SSN is a valuable component potentially in the new account side of things and, hopefully, most folks aren't using the authentication process that my home state did when they -- I'm not even going to tell you what my home state is, by the way, so that none of you can go order my birth certificate

MS. BRODER: We can probably figure it out because we all know your Social Security number.

MR. PRATT: Right, and I’m sure Chip will be able to reverse append in some way to find where I lived previously.

So, the real key is to make sure that not only do we do a good job of using current authentication technologies today, and that's really important, and not only should we use very simple and practical authentication steps, like letting me answer the questions rather than just asking me to say yes to the answers. But we need to expand authentication into a broader range of consequential transactions. It's interesting that Bob used that term, we used that term in our comments to the FTC, we said there's a wider array of consequential transactions.

I testified before the House Ways and Means Committee on the use of Social Security numbers, and right next to me was an individual who said I had a criminal history resulting from identity theft, and I think Chip mentioned a similar kind of circumstance. Well, the answer is that's because many public record creators are not using any authentication systems whatsoever in order to create those records that are then loaded into the public record systems today.

Authentication should occur at the point of transactions like the creation of public records, not just simply the point of creation of records for financial services. That's an important -- that would be a huge step forward for us. To the extent the utilities industry is not authenticating as aggressively as the financial services industry, that should change. To the extent that the telecom industry is not authenticating in the same way that the financial services industry is authenticating, that should change.

In other words, the reality of today is we will go through authentication more often. And over time, as consumers -- I agree, there will never be a single bullet, there will never be a single system, no consumer will trust just a single authority at any given point in time, but we will become more tolerant of the friction that will be at the front end of some of these processes.

I always just fall back on the classic example. You know, when I was a little boy, we used to walk into the airport and walk literally right out onto the -- almost onto the tarmac to watch the planes take off and this sort of thing and, of course, this is when we were taught to duck and cover in elementary school because of a nuclear blast as though my desk was going to protect me. But, nonetheless, this was just a completely different era.

And, today, of course, we walk through metal detectors and machines that puff on us to see if we have chemicals floating around, molecules of chemicals and so on and so forth. We tolerate a lot of things today that we didn't tolerate before, and I suspect over time that we will tolerate yet again a different world and the world will be different offline, if you will. Telephonic, mail, online, in person, those are all different channels.

But I do see some progress, I do see some downward trend. Let me share just one data set. One of the biggest managers of retail credit card accounts in this country did a retrospective on a year's worth of their account openings. So, they looked at 19.8 million accounts opened in a single year. They found one new account fraud for every 1,600-plus new accounts that had been opened, or out of 19 million, somewhere around 12,000 frauds out of 19 million accounts. I mean, you're moving quite a ways past -- you know, towards the right-hand side of the decimal points here. That's good news.

Now, does that mean, okay, we've done it, we're finished, we don't have to work hard any longer? And I think my concern is sometimes that's our discussion that industry is almost implying that if we see a positive trend that we're all going to breathe a sigh of relief and stop trying hard, and that's not true. We're going to try harder. But that is good news, that even the high-speed, what some call the instant credit, but that point-of-sale credit is not, in fact, one of the major drivers of ID theft, the major drivers of fraud. They have found ways to quickly, but still effectively authenticate consumers at the front end of the process.

A great point was made, SSNs are not a sole identifier. I don't know who in their right mind would use a SSN as a sole identifier today. I don't think any of our members would recommend using a sole identifier like a SSN. Jeannine, you and I were on a panel where you said, well, Stuart, it's still being used for an account that you had. Of course, my thought was, in fact, it is true. So, we need better training. We need to train folks to stop using the last four digits of the SSN to access current accounts.

It's a silly practice, really. I mean, that would be the technical term for it. It's just a silly practice and really if you're doing that, you deserve to be a victim of fraud, you really do, as a financial institution if that's how you're going to give me access to my account is the last four digits.

MR. BLAKLEY: But, of course, it's your

customers who are the victims not you. That’s the problem.

MR. PRATT: And, ultimately, customers face this down as well, absolutely. Hopefully, your customers move on to another financial institution that will do a better job of securing your data.

You heard yesterday two great panels that dealt with different ways that the SSN is important to us. It is part of authentication. Bob said it perfectly, it is about linking data together in order to make sure that we're doing a good job of knowing who you are. When it's truncated or eliminated that means we've uncoupled all that data, we can no longer look back into history. But it's different than saying that the SSN is a secret that is being used on its own to go like ah-ha, like my thumbprint, if you will, that this is the ah-ha that's going to authenticate me. Again, that's a silly idea and, hopefully, we're past that.

I think that, finally, though, we're making a bit of progress with consumers, but let me just tell you how many challenges we have as just the average consumer in the marketplace, and I was just penning some of these on the plane on the way home last night. But we need to know about the tools and the toolbox we have, we need to know about fraud alerts and we need to know about access to free reports and we need to know about credit freezes and monitoring services of various types that are out there, and Chip has described one that Intersections provides in the marketplace today.

We need to know about PINs and tokens and we need to know about what types of PINs. I actually met Frank Abignale the other day who was the “Catch Me if You Can," the real live “Catch Me if You Can” fellow, who, in fact, did end up working for the FBI. He said, well, Stuart, what pen do you use to sign checks at CDIA? I said, whatever pen’s in my pocket. He said, well, you know, unless you use this one particular pen with a particular type of ink, then I can just soak the check and all the acetone will just remove the ink from the check and, so, he scared the bejabbers out of me. I’m Blackberrying my staff saying, buy these pens. So, here I am, almost a small business guy using a new security protocol.

So, we need to know what ink we use for checks, we need to know how to shred our paper so when it ends up in the trash it doesn't end up in somebody else's hands, we need to know whether we should have a locked mailbox or not, we need to know whether we should put our bills in the mailbox or not, we need to have ways of recognizing pretexting, and I would say one that's not discussed very often, we need to know more about spyware and key loggers and how to protect our home computers from that sort of thing as well.

So, there’s still, I think, a great challenge ahead of us and, I think, as an industry, we feel responsible for being a part of addressing that challenge going forward. So, I'll leave it with that

MS. BRODER: Thank you. Jeannine, other than going out during the break to change your account that uses your Social Security number, if you could share your thoughts with us.

MS. KENNEY: Thank you. The story that Stuart is alluding to is, a few weeks ago, I was looking to replace my credit card, I needed a replacement credit card with a major issuer, shall we say, who shall remain nameless. So, I called from a phone number, not the phone number of record, and I needed the replacement card sent to a different address, not the address of record, and the only identification or authentication they asked me for were the last four digits of my Social Security number. So, if all the red flags going up in that phone call weren't enough to trigger stronger authentication, I don't know what would, and this is a sophisticated company.

I wasn't reassured by that incident happening to me, but it does give me a good story to lead off on in these presentations because it does really illustrate that as we're talking about longer term, whiz bang, interesting technological solutions to the problem we're confronted with, we have some really short-term needs as well as, I think, long-term needs to protect personal information. It may be the first time Stuart and I have ever agreed that there's really a problem out there right now in terms of the types of methods businesses are using, even very sophisticated businesses, and that has to be resolved with training and training education.

In our view, however, there's really no incentive to provide that training right now. Because I think, you know, Bob mentioned externalities. The externalities of identity theft are really born by other people, not by those who are being lax with your personal data or using inappropriate procedures. And I'm raising this because, Consumers Union has long been working on a number of identity theft solutions, one of them has been giving consumers the right for a security freeze, the right to place a security freeze on their credit file to deter and prevent new account fraud.

We've also been working -- and we've been doing this at a state-by-state level with our consumer organizations as well as working here in Washington.

The other thing we've been working on is trying to get states to require companies that are holding personal sensitive information to notify consumers when that data has been breached, when security has been compromised, even if they aren't absolutely certain that it's fallen into the wrong hands. When it's compromised, the very nature of that sensitive information should be enough to trigger notification to consumers, not based on any sort of subjective risk standard, but the objective fact that the data has been compromised. And we've met a lot of resistance.

The reason we like notice is because it pushes some of those externalities of identity theft back on those holding personal sensitive information because now you can create a market for security. Right now, consumers really don't have any way of knowing who's being lax with their data because only some companies are required to give them notice and the state laws vary to a certain extent. And, so, you might receive notice from your bank because it falls under one particular law that your data has been breached. A local retailer or an in-state retailer may have breached your data, you will never know about it, you do not have enough information to judge which of the businesses you transact with is actually being secure with your data.

So, there isn't a market for security right now at the consumer level because the consumers -- well, there's a market, let's say, but it's not a perfect market because consumers do not have perfect information about who is being secure with their data and who is not, if that makes sense to you.

One of the things I wanted to talk about with respect to Social Security numbers, because they are so important in the ID theft context, was to talk about the results of a poll that we did. About two or three months ago, and we filed the results of that report with FTC and it's available on, I believe, the site associated with the comments with this workshop. We wanted to figure out what consumers thought about Social Security numbers. And I really didn't know how the results were going to come out because I really didn't know if consumers understood the linkages between Social Security number privacy and identity theft, and I was really kind of shocked at the results.

Here's what we found. First of all, that 23 percent of the consumers we surveyed had been victims themselves or had a family member who had been victimized by ID theft. We had at least four in ten believing that information held by private businesses or government is unsafe. Only one in ten believed that the information held about them was actually protected.

We asked if they had been asked for their Social Security number in the last year and nine in ten had been asked at least once, four in ten had been asked to provide it over the phone or the Internet as an authentication, password or identifier. Most of them didn't want to give their Social Security number out. In some cases, you know, they were asked by businesses where you can understand why they were asked, someone extending credit. They were also asked by merchants and retailers not extending credit, and most consumers did not want to give out that information, but they were concerned about the consequences of not doing so.

And sometimes consumers are asked not just by businesses who may want it for the convenience of sorting, but also by non-profits. I gave blood two months ago and my Social Security number was on the donation form, or they requested it on the donation form, and most consumers are going to feel like that's mandatory information that they have to provide and that's basically what we've found. So, consumers get it, they don't want to give this number out, but they feel like they have to. So, when they're asked, they're more likely going to comply.

Nine in ten believe that it shouldn't be used without their permission, and nearly everybody believes that the purchase and sale of Social Security numbers should be prohibited. In fact, you know, if you talk to people on the street, everyday people who really don't even know anything about this issue, most are quite shocked to know that there's no prohibition on the sale of your Social Security number.

And this is perhaps a no-brainer given what we've found in the prior questions, nine in ten believe they're more vulnerable when they give their Social Security number out and most of them wanted laws restricting SSNs. All of them -- virtually all of them wanted notice and virtually all of them wanted freeze rights.

So, I do want to talk about how that information relates to what we're talking about today. One of the things I was asked to talk about was whether the security -- now that we've got the security freeze, 39 states have passed security freeze laws, some are better than others. And, now, Stuart's members have voluntarily made the freeze available to consumers in states where that right is not currently a matter of right by law. And we're asked whether or not that helps with this issue, do we need to stop worrying about Social Security number privacy along with, you know, other sorts of solutions, and my answer to that is absolutely not.

There are a lot of limitations with the security freeze and we have been probably one of the most vocal proponents of the freeze, but it is a very limited solution. As I think someone else mentioned on the panel this morning, it really only addresses new account fraud. It does not address existing account fraud. I was talking with a reporter, I think, from the "New York Times" earlier this week who had her entire bank account emptied. That's existing account fraud and not going to be prevented by the security freeze. And, though, she has a lot of rights under law when that happens, it’s a hassle and there was a period of time in which she did not have access to her funds.

The other problem with the security freeze is that, except for victims of ID theft and with the exception of one state, you have to pay money to place it and, in some cases, you have to pay a lot of money to place it. Many states require a fee of $10 to place the freeze, $10 to lift it temporarily, and $10 to remove it. For a family, say a two-earner family that wants to place a freeze on their mutual credit files and then wants to access credit twice in that year, that's $180 because you have to pay that fee at every credit bureau, $180. So, that's really out of reach for a lot of people, and consumers are going to make a rational choice when faced with those kind of numbers.

What's the degree of risk I face? To a lot of them that's completely unknown because we don't have a lot of market information about the risks that they face because we don't have notice laws on the books in every state or a national notice law. And we think it's going to deter a lot of average people from using the security freeze when, in fact, it's a pretty sound tool to prevent account fraud, though limited on existing accounts.

Second, it's a hassle to place. You have to write a letter to all the credit bureaus to place your freeze. As far as I know, with the exception of laws in two states, the bureaus do not have to give you the right to place the freeze by phone. So, in some cases, the state laws require certified mail. So, you have to make a trip to the post office. So, the rights are very limited. They're expensive. And they really only help with one part of the problem.

So, to us, suggesting that the availability of a security freeze is the reason that we don't need greater protections for Social Security number use, solicitation, purchase, and sale is a little bit like saying, well, we've got locks on the doors, we don't need to patrol the streets, it just doesn't make a lot of sense. We need a range of tools.

So, let me just spend just one second talking a little bit about the legislation. There is legislation pending, two bills in the House reported by the Ways and Means Committee and the Energy and Commerce Committee and one bill in the Senate sort of reported by the Senate Commerce Committee that does address Social Security number privacy. There's a perception that these bills restrict use, and, in fact, they don't. They restrict sale and purchase, by and large. They do restrict display.

One of the interesting things we found on our survey is about one in four people have a card in their wallet that has their Social Security number on it. A lot of those are elderly people, but a lot of them are military people because it's on your military ID card. That has got to end. So, these bills really do some pretty common sense things. You can't sell or buy, except for what are legitimate exceptions. You can't display it on checks. You can't display it on cards and so forth.

There is no restriction on solicitation. The Senate bill has a restriction, but it has so many exceptions to it I can't think of a single thing that wouldn't be excepted. There's no restriction on solicitation. There's no restriction on sharing Social Security numbers, save for a verification, fraud prevention purposes. You're a bank and you have the number and you're accessing a fraud prevention service of an outside vendor who also has that number, and there's no consideration in exchange for that Social Security number, I don't think that's a sale.

So, we've heard a lot about how the legislation that we think takes some really modest steps forward on just some common sense protections for Social Security numbers as we solve the longer term problem, assuming we can ever solve the longer term problem, has really been overblown. I mean, we even heard that this will -- you know, that these protections will increase the incidence of ID theft, that no one will be able to use fraud prevention services, pretty much Armageddon, you know, cats and dogs living together and so forth.

So, that's pretty much what I wanted to cover. I do think that we need to be looking very seriously at more sophisticated tools. I do think that the Social Security number, however, will always be essential for some of the reasons that Bob mentioned and that you can't make it valueless. I don't think it will ever be valueless, and so to suggest that as its value is reduced, as people stop using sort of silly authentication procedures that as that practice ends, we don't need to worry about protecting the number anymore, I think that's really false.

We've got to both look at short-term solutions, long-term solutions as well as more sophisticated solutions to the ID theft problem generally.

MS. BRODER: Thank you. And I'll remind you all that in your packet of information is the summary of the various legislative proposals on the restriction on sale of use of Social Security numbers. So, I commend you to that.

Jeannine, one of your phrases really caught my attention and that is creating a market for security. So, I'd like to hear from those of you on the panel who have something to say about what this consumer experience has been like accepting some of these burdens or increased friction on transactions. Yesterday, Trey French said that, when asked, the customers of his bank said that their first priority is security and only after that it's convenience and whether that's been the experience here with the participants on this panel

So, maybe, Jeannine, since you were just talking, I'll back it up, throw it back to you on -- well, I was going to go the other way, but then it seemed like you were going to talk so...

MS. KENNEY: Why don't you start on that end.

MS. BRODER: Chip, because you're marketing these services and there is some consumer interface, if you can tell me a little bit about what consumers are willing to endure to provide better security.

MR. TSANTES: Sure, and if you've ever purchased one of our products, you have to endure a lot of questions, a lot of information being exchanged back and forth. We do see people drop off at certain points in the process, both online and on the phone, particularly the Social Security number is one that people do drop off on. We've had better success with the last four and we can usually triangulate to your full anyway. But people say things and then do different. So, we have competitors who ask much less information and I would say that they probably have less drop-off than we do. We take a different path where we're going to be more secure and let certain people drop off.

Now, certain people dropping off are, in fact, probably not the individual who's coming in. But others just don't want to be bothered with exchanging that much information to do it.

One of the things that we also do is we run the ITAC for the Financial Services Roundtable and those are people who actually are victims of identity theft, and it's actually a good thing because what --

MS. BRODER: Can you describe a little bit what the ITAC is?

MR. TSANTES: The ITAC is a consortium of banks, and what they do is when they determine that a customer has been a real victim of identity theft and how they define it, they then refer the case to a utility that we run because in almost -- in most cases, people who are true victims of identity theft are victims across -- there are multiple bank relationships. So, instead of having to deal with that incident bank by bank, we run it as a consolidated case, the person can work with one person and work through the problems. It's a good way to do it and it gives the person a better experience because when you're a victim of identity theft, the first thing is call your bank and give up all your identity information that has been taken from you. It’s a fairly thrashing type of experience there.

And, again, in that case, people are willing to give that up, but it’s in a more trusting relationship. The bank has certified that this person is here to help you and that hand-off goes well.

As I said in my opening remarks, I think people are more willing to tolerate security when either they've been the victim of identity theft or when they sense that something’s happening or they’re going through, again, a life change, some event, they've moved to a big apartment building where the mailboxes aren't that secure, something is going on in their life that signals to them that they should be a little more cautious just like if you're walking the streets of New York City versus walking the streets in Great Falls, your gait and your attention's a little different.

MR. BLAKLEY: Well, first, I'll say with respect to these knowledge-based authentication schemes, I went through one of them recently and I missed two out of the five questions and had to be asked extra questions. I suspect an identity thief might have done better and authenticated more quickly than me, but I think that was an anomalous and it may just be a result of me forgetting stuff.

When you talk about creating a market for security you have to bear in mind who the buyers need to be. The buyers of security need to be the people who are creating the security problem; namely, the people who have current problems in the authentication process.

I'll disagree with Jeannine a little bit. I don't think we have to protect the Social Security number because, in fact, the Social Security number is not a secret. What we have to protect is the authentication processes that surround the use of the Social Security number and that currently use the Social Security number in ways that are not appropriate to its nature. The market that needs to be created is a market for authentication of individuals for these various kinds of consequential transactions and that market is defective today because the incentives are wrong.

Let me give you an example of a market where we finally got the incentives right. So, for a long time we've had compliance regulations that deal with security. We had the HIPAA security and privacy rules which resulted in a lot of relatively useless actions, but not really a very great improvement in the security of systems in which personal medical information is stored. We also had the Gramm-Leach-Bliley regulation and the Sarbanes-Oxley regulation and none of those pieces of legislation really created a market for security.

We didn't see an uptake in the purchase of security products to protect private information after any of those regulations that was significant. Where we did see the creation of a market for security was with the intersection of the PCI DSS standard by the major credit card issuer organizations, Visa, MasterCard, et cetera. The reason that that created a market for security was because there were teeth in the regulation that finally put the burden of loss on the people who were creating the security problem, and what PCI DSS did was it said, if your security sucks, we are going to cut you off and you're not going to be allowed to accept credit cards for payment.

And everybody who looked at that said, oh, well, if that happens to me, I will have to go out of business immediately. And, all of a sudden, expenses for security to comply with the PCI DSS rule became an economically rational act. So, I would submit that where the market for security in this particular context needs to be created is in the organizations which are attempting to authenticate individuals for consequential transactions. In other words, at financial institutions and other kinds of institutions that today use Social Security numbers for these purposes and the way to create a market is to ensure that the loss, which will result from screwing that process up, is bigger than the loss that will result from having to buy a product that would enable you to not screw it up

MS. BRODER: Stuart?

MR. PRATT: Just a couple of quick points, one, several different times, I think Bob and maybe Chip as well have made a great point which is as we try to shove certain data back into the toothpaste tube, if you will, to try to protect it and make it secret again.

MR. BLAKLEY: It never was secret.

MR. PRATT: It pretty much wasn’t, that's right. We're probably headed in the wrong direction, but I'm going to divide myself here a little bit. We do think data security is very important. So, I want you all to know that. At CDIA, data security is a very high priority and it’s always going to be a very high priority because it isn’t about protecting a single piece of information on its own, it's about protecting the combination of data because the combination of data is important information, a full and complete consumer report of a certain type.

Obviously, if it's a consumer report based on a public record our thinking is a little different perhaps than if it is private information, if you will, that's been transmitted to us under the auspices of the Gramm-Leach-Bliley Act, a financial institution reporting credit account information. But I think securing data is important overall.

But I do think that the more you uncouple, at least in the short-term until we get to some sort of handheld device I guess that allows me to authenticate myself in a different way in the future, at least for a period of time, then more data will be demanded at this point in the transaction to try to authenticate who I am.

So, one of the great ironies is if you take the Social Security number out of the -- as a linking mechanism, you're actually forcing me to give more data to the person on the other side of the counter at the DMV, to the person on the other side of the counter in the retail context, to the person over the phone or whomever I'm doing business with, because now they need more kinds of data to try to find some connection, to try to see if I am who I say that I am. So, we want to protect the combination of data, the SSN plus other dates of birth and other kinds of data. Of course we do.

And on the other side of it, we want to have that data, but we don't -- this is really so important to this process that you put together, this dialogue is a great dialogue, Betsy, because we begin to pull apart the difference between using data effectively to authenticate and prevent fraud versus using data as a secret to authenticate me, you know, account by account either on the new account side or in the account, managing me on a go-forward basis.

We probably should just move away completely on the current account side from allowing us to choose mother's maiden name or things of this sort. There should always be a really unique question and they’re starting -- some best practices are out there, what was the name of your first dog? Which is going to be a hard one to track down. It's probably not in the public records somewhere. Although -- and I wasn't asked that by my home state when I disclosed my --

MS. BRODER: Well, they knew it already.

MR. PRATT: They knew it, right. But a birth certificate, it has your mother's maiden number. A birth certificate has where I was born, the county in which I was born, lots of things in it, and public records are public records for a reason in this country and there's good reasons for public records. But we shouldn't use that set of data as the secret data, if you will.

So, as you move away from the authentication process with the new account, then you should establish a different relationship with the consumer which is dis-intermediated, which is separate from the next account down the road and separate from the next account down the road.

We are empowered, as consumers, when we have that kind of opportunity with our financial institutions, with our utilities, with our -- by the way, one of the great questions is going to be, how are we going to do when the real ID act is really effective and we're all showing up at the doorstep of DMVs all over the country, who has done the background screening on all these folks when I'm dumping all that data onto the counter top, including birth certificates, and they now have that data?

The majority of breaches in this country, if you're going back to breaches, have actually occurred with public agencies, government agencies losing more data and more sensitive combinations of data than the private sector, and, so, I don't feel good about that at all. But they should have good authentication, they should be buying -- I don't care whose product you buy, but they ought to be buying good authentication and they ought to be under the same data security standards as the financial services industry is today, as our members in the CDIA are today because good security is a good thing.

And, by the way, the state laws do create incentives, they create safe harbors for practice. If you’ve truncated data, if you’ve rendered it unusable, you no longer have to notify because you’ve rendered it unusable, it’s no longer valuable to the identity thief. So, there are ways that law will sometimes leverage a little bit the practice. We think we've gotten there, by the way, with a lot of state laws today even with breach notification.

MS. BRODER: Just in a plug for the Task Force recommendations, one of the recommendations would be that there will be federal legislation requiring breach notification when there is significant risk of identity theft. So, even though there is that void now in certain states, we recommend that that be taken care of.

Jeannine, since you were one who authored the phrase "creating a market for security."

MS. KENNEY: Thanks. Let me talk a little bit about the notice of breach and sort the different incentives that we think that -- the different approaches notice of breach can take because I think it really is relevant for the market for control.

Bob said, I think it was Bob, said, look, you create incentives when you know that the cost of not screwing it up is going to be less than the cost of screwing it up. In order to know the cost of screwing it up, though, you have to know what the consequences are. And, so, breach laws that create uncertainty about whether or not you will have to notify and give your legal counsel opportunities to argue that the risk isn't significant or the risk isn't reasonable or whatever the risk threshold is that triggers the notification, you don't know for certain that you're going to have to notify and, so, you don't have the incentive to necessarily invest in the technologies that will prevent a breach and improve your internal and external procedures.

If you know that unquestionably when this subset of data is breached, the subset of data that is inherently risky, whether it's your Social Security number or other secrets that are used to authenticate you, you will have to notify you know what that number is, you know what the cost of notification is going to be in terms of the number of consumers on which you hold data, and you also can probably estimate the loss of good will, which is a significant threat for at least those entities that transact with the public and potentially for all entities.

So, we would reject the Gramm-Leach-Bliley standard which is actually a trigger notification. The strongest incentives are created when you can accurately assess what the costs of notification are going to be and then you know whether or not it makes more sense for you financially to invest in technologies. If you don't know that, I don't think you create a market for security.

MS. BRODER: I think Bob had something to say and then Stuart and then think about questions because we'll turn it open to you.

MR. BLAKLEY: Yeah, I think that's exactly right, and one of the things that I was originally trying to say, but I think maybe didn't make explicit, was that when people talk about creating a market for security, they shouldn't talk as if they are going to create incentives for individuals to buy security products. It's the organizations that put data at risk that really need to be in this market.

I did want to just draw a little bit of caution about something Stuart said. You referred, Stuart, to de-identification of certain records and sort of rendering them safe so that they can easily be disclosed. I think it's a good practice to try, but I'll just warn that one of the lessons of AOL's misadventure is that actually de-identifying a record, unless it's very strongly structured, is much harder than it looks, and I think even the HIPAA privacy regulation acknowledged that by making you, if you're a big institution, hire a statistician to tell you whether you've screwed it up. So, I really want to caution people that de-identification is something that’s best left to serious professionals and that, you know, you should not assume that you've ever done it.

MS. BRODER: Do not try this at home.

MR. BLAKLEY: No.

MR. PRATT: And, by the way, unusability was the term I used and that's a broader term than de-identification. I suppose you could assume that that's one route. It could also be various methods of encryption, various methods of scrambling and doing other things to the data.

Now, I understand from a technical perspective, if somebody's smart enough and has enough horsepower computing-wise, maybe they can break down some of that. Everything's going to operate on a continuum from not very good at all to very, very, very good.

MR. BLAKLEY: It's better to do all of those things than not to do them. It’s also better to be careful about your assumptions.

MR. PRATT: Absolutely, absolutely, I’m going to defer to my subject matter experts on that.

My only point here was that case law today is also another voice in all of this. So, I understand what Jeannine is saying about needing incentives, but keep in mind, retailers are being sued by banks today for the retailers' loss of account numbers. So, the only metric by which an in-house counsel is evaluating notification and data security and authentication is not just the breach notification law and whether or not it has an incentive to somehow protect data, but it's also the case law that's out there today.

So, retailers today, and others who have data, know that they have -- and, by the way, some CDIA members are even facing class action lawsuits right now outside of what they did or didn't do, and choosing not to notify can give rise to class action lawsuits as well. That is a chaotic case law context. Don't you like that alliteration? But nonetheless -- you can use that later, Betsy.

But the bottom line is there is a judicial context for the decisions that are being made, not just simply a statutory or interpretive context. In the real world will I be sued, who might sue me, is it the folks from whom I purchase the data, is it the consumers whose data, if you will, has been lost or put at risk in some way, in addition to notification laws and so on and so forth.

So, I'd say there's a lot of layers in there today and it isn't exclusively this one binary, do you notify, do you not and are you okay, are you not.

MS. BRODER: And I think Jeannine's point was that it needs to be clearer to the company that holds the data what these externalities are and that there is uncertainty out there from state to state and by data to data set. So, I think we're all maybe close to agreeing, I don't know.

MR. PRATT: Yeah, I think that's pretty good.

MS. BRODER: Chip?

MR. TSANTES: Just two quick points. Bob's lucky that actually he missed a couple of questions. When someone answers all the questions right, we're usually suspicious because usually it’s a fraudster who’s done the homework to do that. Just to follow up on what Jeannine said, some of it’s technology, but I would say we provide breach mediation services to people who lose data, and in almost all cases, a human is somewhere involved in the breach. So, if I had one dollar to spend on security, I would spend it on training.

MS. BRODER: I think we all agree on that, too, particularly in Stuart's home state.

I know that there are a lot of people getting up to ask questions, so our team will reach out to you. Please raise your hand and we will take your questions. I need someone with a mic to go someplace. Lael?

MS. BELLAMY: I just wanted to respond to the concern about retailers since I think I'm the only retailer in the world here. I think that the notion that retailers aren't doing anything is completely false. We work very closely with our trade associations, NRF and RILA. Every retailer I've talked to has been working on privacy for years and years. The state of the data breach laws don't have anything to do with how important we take not only the consumer's privacy, but our employees' privacy, and that's something we haven't spent a whole lot of time talking about here. But retailers are some of the largest employers in this country and we feel deeply about the privacy of both our employees and our consumers.

I mean, there are what 42 odd data breach laws. We look at every single one of those. We always err on the side of trying to notify people even when there's a question on whether or not there's risk. You always try to do the right thing. There are plenty of state laws which require you to notify even if there isn't a breach law in that state because of deceptive practices or potential harm or negligence. So, we go out of our way to do all those things. And, you know, you need look no further than the paper to realize that TJX and all these companies have experienced terrible losses, and it's definitely in the forefront of people's minds.

So, I just want to put that forward to let you know that we do take this extremely seriously and we have for a very, very long time.

MS. BRODER: Thank you. And I think it was helpful also to get the structure of short-term and long-term issues out there. Yes, Jim?

MR. McCARTNEY: My name is Jim McCartney with

Bearing Point with the DoD.

Jeannine, to answer your question, the SSN is coming off the military ID cards. There's a plan that’s in place and working towards that. It will take a while, but we'll get there.

MS. KENNEY: Excellent.

MR. McCARTNEY: Bob, you made a great point about changing -- already knowing where you’re changing to before you move. I think it goes to a bigger question of unintended consequences, that whatever action you take, there's going to be some kind of consequences and to better understand what those are is a key thing before you move. But I’m not saying we shouldn't move.

I like your comments that, you know, the pain of remaining the same has to be greater than the pain of movement before we get going, and you also talked about that in terms of financial data.

My question is: What do you see besides federal legislation or state legislation as options to make people understand that the pain of remaining the same has to be greater? So, what could you see other than that, to do, that? I know PCI certainly had some way to do that, but I'd like to know what your thoughts are going beyond that.

MS. BRODER: And I'd like also -- Bob, it was directed to you -- but for Jeannine to respond as well to that question.

MR. BLAKLEY: So, I'll go first and I'll go relatively quickly. First, I wanted to say to Lael's point that I don't remember anyone saying that retailers don't care about security and I don't believe it's true that retailers don't care about security. They sometimes don't do it as well as they should and that is partly because vendors who provide them with products don't do it as well as they should and partly because it's hard to justify expenses for security in the absence of quantification of loss. So, I certainly don't want to pin this on retailers.

To respond directly to the question, the classic problem with an externality is that it requires some sort of intervention to make the market function as it should. That's often a government intervention, but it doesn't have to be. PCI DSS was imposed essentially by the financial industry, by one portion of the financial industry on another, and the forthcoming PA-DSS regulation will impose the same burden on merchants as has been imposed on payment processors and others, and that will certainly go some way toward reducing an externality.

But, generally speaking, a rational business will always lay off costs for which it is not liable on either its customers or other parties. And, so, the way to prevent that is to make sure that the liabilities don't allow that laying off of loss and whether that is industry sector action or government action, it's got to be somebody's action or else it wouldn’t be an externality in the first place.

MS. KENNEY: I don't know if I could put it any better than that. To be frank, we don't really see a viable solution other than forcing change on the industry, and I think the howls of protest that we received both on restrictions, on purchase and sale of Social Security numbers, on strong notification laws, on security freeze even, for a very long time, across all sectors, all sectors of the economy, it's put very clear to me that this isn't going to happen voluntarily. Businesses aren't going to take these externalities on themselves.

Stuart raised the interesting question of private lawsuits. The reason you don't see more class actions on breach is because it's extremely difficult to establish sort of the basic tort elements for these types of harms. Because you're going to have a difficult time showing causation linking the breach to some economic harm, and if you didn't suffer a harm, physical or economic, you didn't suffer any damage and you don't have a cause of action.

So, I would be very interested -- we certainly have heard enormous protests in creating a private right of action for security breach at the federal and the state level. But if industries are willing to accept that, I think that is another way to go in terms of creating incentives because right now I don't think consumer class actions are much of a threat perhaps in the business world. They may be business-to-business suits, but, really, it's very difficult for consumers to recover from these types of harms in a court of law.

MS. BRODER: A short response from Bob and then a question in the back.

MR. BLAKLEY: And I really don't like private rights of action because essentially they place an additional burden of effort and cost on the individual who has been harmed to go out and hire a lawyer and do all this affirmative stuff when, in fact, the right thing to do would have been to put the burden of not causing the harm on the business in the first place. So, I think individual right of action is great if what you're into is anger management, but in terms of creating a market it's not that great.

MS. KENNEY: I’m not going to disagree with that, by the way.

MS. BRODER: We have a question in the back.

MS. CRABTREE: Hi, I’m Jamie Crabtree and I’m with First Advantage Corporation. We are a member of CDIA. And I don't think I could say it better than Stuart did with regard to risk assessment that goes on in the boardroom because, certainly, I’m a piece of that at my company, being an in-house attorney, and I can tell you that there's nothing about making breach notices automatic that would make us be any more secure because we already do a lot of things that are just industry-driven, including getting assessments from third-party security firms and certifications, and I don't think that that would at all impact our security assessment because we already know how many zeros go after that loss, at damages awards on those lawsuits.

MS. BRODER: Thank you.

MR. PRATT: If I could just add to that, on the security side of things, Betsy, which obviously ties back to Social Security numbers as one part of the set of data that you're securing, we've actually gotten to the point where we're getting phone calls from the customers of our members angry about the levels of credentialing that we're doing, the password management strategies that we're rolling out. And, so, the irony of it is we're actually -- there is an enormous amount of pressure in the marketplace.

I would just push back on the idea that there's no movement in the marketplace, that the marketplace today doesn't feel the pain necessary to move forward. The marketplace is enormously large and it's going to take a lot of time to turn the battleship, if you will, for every single entity that’s out there that has -- whether it's processing a credit card or processing a consumer report. But the incentives are enormous today, within these companies, all the way up through the board level.

MS. BRODER: And I would suggest that if they weren't there, these two gentlemen wouldn't be in business doing what they're doing.

MR. PRATT: That’s true.

MR. BLAKLEY: And, you know, it's not the point of creating a market to improve the performance of the best players in the market who, by and large, are the people who come to meetings like this, right? There are a lot of people out there who do a very good job and they're the ones who are your members. There are also a lot of people who don’t do a very good job.

MR. PRATT: I think we need to do more training. This has been said several times. We have got to get out into the marketplace and penetrate more deeply and train more people and impose more good data practices through the software we roll out into the marketplace.

MS. BRODER: And the overlay of everything that we've been talking about yesterday and today is the assumption of good, strong data security, and what we're doing is building on to that short-term/long-term issue.

MS. OLNES: Hi, I'm Karen Olnes from Wells Fargo. I have a question for Jeannine and others, if you'd like to weigh in on it.

Could you elaborate on your idea around what should be included and excluded in the definition of purchase and sale of SSN?

MS. KENNEY: Sure. I think the biggest fight has been over -- and I don't -- let me say that I'm characterizing the problem this way. I don't think others have, this is my perception of what the problem is. There is concern among, I think, Stuart's members, the financial community, obviously, that if you can't buy or sell the SSN, you can't use fraud prevention and verification systems because the SSN is such a crucial component of those, which I think undermines the argument that, in fact, the SSN either isn’t or shouldn't be that valuable. It clearly is very valuable right now to these processes or people wouldn't care, right? They just wouldn't care if you couldn't buy or sell the assets and if it wasn't an essential part of these systems.

But I think the concern is that there are some businesses that hold the SSN already, right? You're a creditor, you've got to ask for the SSN, you're going to do a credit check, and you may also be using some fraud verification system, either with an affiliate or an outside vendor. At least as I'm interpreting some of the concerns I have heard third-hand, and I would be very open to a discussion with the industry about this, because I do think this is a solvable problem, I don't think we believe that if Wells Fargo has a Social Security number and is using an outside fraud verification system and it provides the SSN for matching purposes to the verifier or the outside service, whatever the service is, and no SSN, so both parties have the Social Security number, I don't think that's a sale. I don't think that's a purchase.

That's sharing. There's been no consideration exchanged for the Social Security number. You may have paid for the service, but you both already had the Social Security number. So, as long as the outside service doesn't send you back someone else's Social Security number, you haven't bought anything, you haven't bought the Social Security number.

So, to the extent that we can address that problem, those who legitimately hold the Social Security number, I don't think should be constrained. Now, there are a lot of businesses who seem to collect the Social Security number that don't appear to need it and they shouldn't be selling that number to another party. That's shocking to consumers that, you know, the blood bank could take your Social Security number and sell it.

MS. BRODER: Jonathan Cantor and then Beth Givens.

MR. CANTOR: Hi, Jonathan Cantor, I’m with the Social Security Administration. I just have a couple quick comments because I heard a couple things about ideas involving the Social Security number that I think I need to clarify. At one point, there was a discussion up there about we can call or mail things to the address of record for the Social Security number. One of the problems is is that Social Security as an agency, we interface with people at certain kind of key points in their life and one of those is when they get a Social Security number, and then, in many cases, we don't see that person again until they file for benefits. So, we don't actually keep track of people's addresses and we also don't keep track of people's phone numbers.

So, there's kind of a hidden cost that falls onto government right now which is not currently funded and, you know, there's a cost associated with that which would fall to all taxpayers to sort of increase the infrastructure that would support that.

MS. BRODER: Could you speak more clearly into your mic, please?

MR. CANTOR: Okay, I was talking about the fact that the kind of costs -- you would have increased costs of asking Social Security to maintain the addresses and phone numbers, which we don't currently maintain, if we're the only ones with the complete set, for lack of a better term, of the entire database of Social Security numbers, then this idea of having Social Security or having some ability to contact the address of record or the phone number of record of a Social Security number holder falls directly on Social Security to maintain that information, and we don't currently do that, so somebody would have to fund that activity which is obviously going to have to be taxpayers.

And another comment came up about Hurricane Katrina, and I just kind of wanted to point out that, you know, people are saying, well, Social Security numbers were the only thing that they had. A lot of people who were victims of Hurricane Katrina also didn't have their Social Security numbers available and they didn't know what they were. So, there's a lot of people in this country who are not participants in the economy to the same level as a lot of other people. And a lot of those people aren't really engaged in many agencies or working with anyone. So, the availability of the Social Security number to those folks is also limited and they, after Hurricane Katrina, didn't know any of their identifiers other than their name.

MS. BRODER: Thank you.

MR. PRATT: Betsy, could I just put context around that? First of all, in the context of Katrina, it was the government who then turned to the private sector to, in fact, connect the data back together to allow consumers to identify themselves and so it was the third party databases built based on the kinds of data that we're discussing, including the SSN and the private sector, which connected consumers back to what they needed in the context of Katrina.

Also, I don't know who suggested that the SSA was going to be the oracle for all identifying information, but the SSA could certainly verify that Stuart Pratt, Stuart K. Pratt and an SSN, that combination of name and Social, exists. You may know nothing else about it. You may not even know whether it's truly a citizen --

MR. BLAKLEY: Date of issue.

MR. PRATT: Well, date of issue, you could make some guesses about that. But I’m just simply saying that even that combination could be part of a full and complete identification process.

To clarify what Jeannine is saying, again, Jeannine, we're not saying the SSN is a secret and that's why it's important. We're saying the SSN is a mediating link and that's why it's important. So, it's important for fraud prevention, not for facilitation of the application approval in a sense. So, I just want to make that clear, that it's about looking to see if we can find a reason to have a yellow flag or move towards a red flag or to identify 10 yellow flags which together require more questions to be asked of the consumer directly.

So, we see it as a positive from that perspective and that's why it's important and that's why we still think it's a valuable tool in the marketplace. But it's not a facilitator of fraud in the sense that it's a secret which is used in combination with a name, and if I have your name and your Social, thumbs up, there you go, we've opened the account. If that's happening today, that's a training issue.

MS. BRODER: Jeannine and then --

MS. KENNEY: We keep hearing how the Social

Security number is used. It's important for this, but not for this. I mean, maybe those entities that are using best practices are doing that. But we clearly know that's not what's happening out in the marketplace. To the extent that we can structure regulations, new restrictions that can address legitimate needs for the Social Security number, but eliminate those that are unnecessary, the uses that are unnecessary, the exchanges that are unnecessary, I think we get pretty far.

The problem is we haven't been able to have that discussion. I mean, there may be in an asymmetrical restriction on sale and purchase that might be appropriate if, in fact, it is really essential as a linking element but is not used for authentication. But if you're going to have a provision like that, it's got to come with some regulatory strings because you have to be able to hold those who are claiming they're using the data for a particular purpose are, in fact, using the data for that purpose and no other, a little bit like the Fair Credit Reporting Act where there is a regulatory structure around it

MS. BRODER: And we can probe this more on the last panel on recommendations. Beth Givens, I think, had a question.

MS. GIVENS: Yeah, I do, it's for Stuart.

MR. PRATT: Hi, Beth.

MS. GIVENS: Hi, Beth Givens, Privacy Rights Clearinghouse, Consumer Advocacy Organization. When I give speeches -- I’m kind of changing a little bit what we've been talking about, but when I give speeches it’s mostly to seniors these days and I give my top 10, the top 10 things that every consumer needs to know to protect their privacy and prevent identity theft. The most popular tip I give is how to opt out of receiving pre-approved offers of credit.

Many people receive several offers in the mail of pre-approved offers of credit each week and many don't know that there's this opt-out. It’s 885OPTOUT is the phone number to call, and you can also, by the way, opt out online. I think it's optoutprescreen.com.

But for older people I think they're more comfortable on the phone, calling in and opting out that way and it is an automated process, but going online kind of unnerves them. The problem is on the phone the Social Security number is asked for and that is a big barrier. People stop at that point, choke and say, oops, I better not opt out. I'm wondering why couldn't you go to a last four. I think there's a social good to reducing the number of offers of pre-approved offers of credit that flow through the mail which could then be picked up by a mail thief, an identity thief, fill in the blanks, find out the SSN and get credit that way. And even if it doesn't happen that way, the perception is out there that it does happen that way.

I think consumers would be far more comfortable if you just wouldn't ask for the complete Social Security number, maybe ask for a date of birth in addition, but I'm tossing it out as both a question and a suggestion on the phone opt-out option.

MR. PRATT: Thank you, Beth, for saying it the way that you said it with regard to pre-screening. I do think there's more urban myth than reality around pre-screening as being an easy focal point of fraud. In fact, the data coming out of the big financial institutions says that pre-screening is one of the least exposed areas of fraud when it comes -- just so you know. That's different than a perception that may be out there. So, Beth, I appreciate the way you’ve said it because perceptions are important and consumers hold those perceptions. Dialogues like this allow us to maybe push the needle back towards the middle a little bit.

With regard to the Social let me just say it this way in terms of why we want the Social -- and I'm always happy to have more discussion about how to then, along with our members, of course, it’s our members who run the system, not the CDIA. But we’re happy to have a dialogue with our members about things like how to make sure it’s a system that's friendly to consumers.

The reason for all of you who are here in this room and all of you that are listening out there in Internet land is that we're obligated to find just the right record in the database and make sure we really opted you out so you don't get those offers if that's what you want. So, the full Social allows us, particularly with a John Smith or a Jeannine Smith, who's moved recently or divorced, to still be able to identify that consumer. And if we don't identify the consumers on a regular basis or fail to do so, it's Joel Winston and Betsy and others who then come to our doorstep and ask us why we're failing to properly opt consumers out.

We probably don't need to have all of this discussion here in the room. I'm happy to catch you as we leave the room to talk a little bit more about truncation versus full Socials, whether that's an impediment or what we could do to communicate effectively with consumers

MS. BRODER: We have time for one last question.

MR. HULME: How do you do, I’m Bruce Hulme. I’m the Legislative Director for the National Council of

Investigation and Security Services, and I speak here for 60,000 licensed private investigators and quite a few large regional contract security companies.

Yesterday, one of the speakers from Acxiom, when talking about medical ID theft, indicated that it was a lot more than just the financial implications and, of course, it has to do with the manner of the procedures and life. I just want to point out as we're talking about the Social Security number, from our standpoint, there's more than just the economics, it's also the people, now and then, that are freed from jail, that have been -- witnesses have been located with the use of this number. It's frauds, elder fraud cases that have been solved by the use of this number.

I was surprised to hear Jeannine say that she doesn't think that the legislation proposed would necessarily impact on this sale aspect or display. We're against the display of the Social Security number on many documents. We are for Draconian sanctions against those private investigators and independent operators that do what I heard, the ten indicted, well, if they're convicted, fine, throw the book at them. We’re willing to pay the penalty.

At the same time, we are a regulated industry to a degree or a profession to a degree and we only speak here for the regulated people. So, we would go back to the sanctions. But at least we're vetted, for whatever it's worth. And I would like to just read something from the International Association of Security and Investigative Regulators, those are the people that regulate our industry. In their letter to Congress, basically, they urge that regulated licensed private investigators continue to have access to Social Security numbers and other identifying information.

I handled a case for the courts in New York. I'd like to point out that there's an eight-page memo that was submitted and I hope that everybody here gets an opportunity to look at it from the National Council of Investigation and Security Services. It outlines the horror stories, and those horror stories that in those investigations justice prevailed on the basis of accessing the information that led us to the witnesses, and it was through the Social Security number.

We don't care what identifier is used as long as we have access to the same thing that links all of these sources of information together so that we can locate where this individual is. I thank you, and I'll be hanging around for any questions anybody has.

MS. BRODER: Any comments?

MR. BLAKLEY: I'll make one comment. We

certainly have no objection to, for example, federal and state police using Social Security numbers in investigations. And I think on that basis my opinion would be that as long as due process is observed, if the legal system chooses to subcontract some investigative procedures to private entities, then there seems no reason to inhibit their use of effective tools in cases where it could lead to better justice being done.

MS. KENNEY: If I can respond since I think that was largely directed at me, I would agree with that and there are exceptions in these bills, strong law enforcement exceptions, that I believe would encompass private investigators acting under color of state law, for example. And, so, those, I think, are fine, legitimate needs for a Social Security number and they are accepted under the bills that are pending.

MS. BRODER: Thank you. Maybe you can follow up during the break. So, that will be the last word on this panel. Thank you all very much for a very engaging conversation.

We'll be taking a break now. Please be back promptly at a quarter till 11:00.

(Applause.)

PANEL 6: RECOMMENDATIONS

MS. RICHARDS: All right, well, thank you all again for coming. This is Panel 6, and in the next two hours, we will solve all the problems related to identity theft.

So, joining me today for this panel, Chris Hoofnagle, who you all heard yesterday. He's kind of our bookend panelist and is a Senior Staff Attorney at Samuelson Law, Technology and Public Policy Clinic at UC Berkeley School of Law and, also, Senior Fellow, Berkeley Center for Law and Technology. He’s focused on privacy law and talked yesterday about synthetic identity theft.

Fred Cate, Distinguished Professor and Director for Applied Cybersecurity Research, Indiana University; Senior Policy Advisor, Center for Information Policy Leadership, Hunton and Williams. He serves on boards, he’s authored books. All three have authored articles, books, and journals. And, also, is an expert on privacy and security.

And then Jim Lewis, Senior Fellow and Director of the Technology and Public Policy Program, Center for Strategic and International Studies. Had a prior federal career, National Security and Technology.

So, we will start with our panelists doing presentations and then I will ask a couple questions and then we will turn it over to the audience. This is the recommendation and the solution panel. So, if you could think about those recommendations you'd like to make to us, this is your time to do that.

And with that, I will turn it over to Chris.

MR. HOOFNAGLE: Thanks, Mary Beth, and thanks, again, to the Federal Trade Commission for putting together this useful workshop. I know it's a lot of work to do one of these meetings and to put together panelists who can talk substantively about the issues and I very much appreciate it.

Let me start by revisiting some of the issues we talked about yesterday. We started with John Webb who said that Social Security numbers and identity theft go hand in hand, that Social Security numbers are a key component of any financial crime. In some jurisdictions, you have to engage in a huge amount of fraud before the federal government will even investigate. So, he gave the example, L.A., that you'd have to steal $750,000 worth of assets or have some other kind of mitigating factors to get the U.S. Attorney interested in a case like that. He also said that pre-approved credit offers are still a problem.

Bob Sullivan said pre-approved credit cards are still a problem. In his comments, he talked about the situation where someone ripped up a pre-approved offer, taped it back together, mailed it in and still got the card at a different address. He talked about the credit card being issued to Don’t Waste Trees, someone named Don’t Waste Trees.

At the same time, there's a lot of tension here because Lael Bellamy says, reputable retailers do a lot, and I believe her, I think she's right. Reputable retailers do a lot to deal with the Social Security number and some of the authentication problems there. But maybe some of the bad actors aren't in this room. I think that's one of the messages we should think about is that maybe the good actors are here and some of the ones who are doing not such a great job don't make it to these types of events and maybe they’re not spoken for at these events.

Panel 2, we heard about how companies needed the SSN internally and to interact with others. Jim Davis, you know, he basically runs a small city at UCLA. They do health care, they do financial, they teach people, they pay people. He's got about the most complex situation that can be possible out there with regards to the Social Security number. Yet, they were able to transfer their internal systems over to non-Social Security number infrastructure and it took them about two years. He said it wasn't hugely expensive, but it was process intensive.

He was followed by Bill Schaumann from Ernst & Young who was kind of in accord. He basically said, this can be done but you need executive buy-in, you need buy-in from the top to push these policies down through the organization. Because so many people will say we need to use the SSN, that's how we've always done it.

Panel 3 is, I think, when things got a little bit weird. We seemed to get two different messages. On one hand, people were saying the SSN isn’t so important, but on the other hand, they were saying if you take it away from us, bad things are going to happen. And Robert Townsend made the great point, if the SSN isn't so important why is it so tied to the idea of identity theft? Why are licensed investigators so pursued over this issue of the SSN if it isn't important?

Professor Anton also talked about a way to use software to reduce reliance on the SSN to mask it in databases.

So, we went on to Panel 4 where we had all the tension in Panel 3 about whether or not the SSN was important, but then in Panel 4 the SSN was in the center stage again, right, the SSN was the key factor for high-risk transactions, and the good news is that it's being used less in low risk transactions but, you know, when you're applying for a loan, you're doing anything with the credit reporting system, that SSN is going to be there and, of course, the credit reporting system has gone down and down into even smaller transactions. So, that means a lot of SSN use.

We also heard from Thomas Oscherwitz from ID Analytics who said that other data could be more predictive. The SSN helps them, removing it would harm their ability to predict frauds, but other data, in fact, are more predictive.

Then we heard from Trey French who, among other things, said that they approve 14 million credit applications a year at Bank of America meaning that they are processed by computers, not by people. That might explain some things.

I'm not going to go over Panel 5 because we just heard it, but I did want to point out that Chip from Intersections pointed out that the more authentication you ask for, the more drop-off you have. So, there's also a market incentive not to engage in some authentication, I think, is one message that you can take away from it. So, obviously, it's a bit of a balance.

The reason why I mention these tensions is that in the research I do on identity theft, we keep on finding examples where there's only SSN matching in credit granting. So, in the most recent case, this is Western District of Tennessee, Wolf versus MBNA, for those of you who want to look it up, it's 485 F.Supp 2D 874.

An MBNA telemarketer, because as I said, this was not an in-person transaction, approves a credit card for someone and nothing matches. This credit card is given to a 21-year-old without a job who has a $55,000 salary on the application. Date of birth doesn't match. False address. Phone number doesn't match. The nearest relative is not a relative of the victim. The credit card is issued anyway. And in discovery in that case, the plaintiff's attorney got a document from MBNA saying that nothing was verified, that is a direct quote from MBNA.

This is actually a solution, this case, and if you look at this case, this is the first, to my knowledge, in the nation where a judge has held that a bank can be liable in negligence for credit-granting to an imposter. And, so, this case stands for the proposition that at least in Tennessee -- and we have cases going the other way in other states -- one can sue a credit granter for negligence.

And I think this is -- you know, I don't know what gets more negligent than that. I think when the red flag rules come out it's going to provide another basis for determining negligence.

But there's other cases that have occurred over the years. Vazquez, a lot of stuff didn't match. This was a case where the imposter applied for credit in Nevada, but the victim lived in Puerto Rico. TransUnion was the defendant in that case. Aylward that was Fleet Bank and Dimezza First USA Bank. Let me point out that in their comments to this proceeding, the financial institutions as a group said that they wanted to use the SSN, which is fine, I think it's probably reasonable to use the SSN as an identifier, but they said explicitly they want to use the SSN as both an identification and a authentication. It's in the same sentence, identification and authentication.

So, I think this leads to a lot of ways we can go. I think there's solutions for every actor in this field, but credit-granters are really in the best position to avoid theft. They're the ones who are deciding whether or not to buy enhanced authentication products that are offered by all the consumer reporting agencies that we heard about from ID Analytics, that we heard about from Acxiom yesterday. They're in the position to buy those and they can either use them or not and they can either follow the recommendations or not.

The victim is in a position -- I mean, look at the guy from Puerto Rico. How could he have stopped a credit lender in Nevada from granting credit in his name to someone who didn't even have the right information?

It's clear that more than the SSN needs to be matched and the SSN should not be used as the authenticator, which brings me to the red flag guidelines which are really interesting. If you look at Appendix J of the red flag guidelines which, by the way, I think are really going to help and I think we might be in a very different place a year from now because of red flags. It is a red flag if someone applies with an address that does not appear in the credit file, but if you apply with a false name, it's not a specific red flag, at least it's not enumerated in Appendix J, which I think is an interesting problem and it's something that the Commission should visit.

Consumers do have some approaches. I'm going to work very hard on negligence suits because I actually think that that is what can bring more rationality to the situation. I think it is a way to shift more of the externalities on to the companies that are lending to obvious imposters.

Also, in the self-help field, I think it's important that -- you know, there's a whole menu of options one can consider now. There’s the fraud alert. I think the problem there is that some people ignore it. And in FACTA, if you read FACTA, consumer reporting agencies have to offer the fraud alert, but retailers don't have to follow it on a sharp reading of the law and that, I think, was an oversight in the FACTA.

If you look at data coming out from Identity Theft Resource Center, they’re saying about 20 percent of their victims were victimized after they placed a fraud alert, meaning the fraud alert was ignored or defeated.

There's also credit monitoring out there. Of course, credit monitoring does not prevent identity theft. It also doesn’t deal with the emerging problem of synthetic identities. So, I think one great self-help piece of advice here is coming from Avivah Litan and that is to move towards identity scoring rather than credit monitoring as a way to see whether or not your personal information is being used.

And it would be absolutely awesome if the consumer reporting agencies created tools for consumers to buy. There's a lot of things that consumer reporting agencies can do. I don't have time to go over all of this stuff and I think some of it is perhaps obvious.

But let me just make two points from the slide. One is is that the add-on products, all the consumer reporting agencies offer these enhanced authentication products that some credit granters are not using. We should think about whether that's a good idea. And it would make sense to do a study to see the relative fraud rates between companies that have good practices; for instance, it sounded like Bank of America has pretty good practices from yesterday's presentation, and everyone else out there to see if these add-on products are effective and whether or not they should be a default in credit granting.

And then the last recommendation here, I think a couple years ago might have sounded totally unreasonable. But with the advent of credit monitoring and millions of consumers signing up for credit monitoring, with the advent of annualcreditreport.com where people are going online and getting their free credit report, we really are coming to a point where consumer reporting agencies can have a one-to-one relationship with consumers and for there to be more mutual communication between the two, where there will be more accuracy, more understanding of the practices.

Remember that the Fair Credit Reporting Act passed in 1970 because there was no consumer relationship with consumer reporting agencies. It was a way to fix a market failure. Former Chairman Tim Muris used to note this. He used to say the FCRA was one of his favorite privacy laws because it rectified this imbalance, this lack of relationship and lack of competition.

I do think that we're going to a point where we could have harder relationships between consumer reporting agencies and individuals. In fact, if you read Dan Solove's article, Identity Theft, Privacy and the Architecture of Vulnerability, he proposes a situation where when you're 18, you go and you choose a consumer reporting agency and you create a relationship with them. You could do in-person proofing to prove who you are, and that way, you could actually have competition among the CRAs from consumers themselves, and if Experian has better practices than another consumer reporting agency, you could sign up with Experian, et cetera, and that could change over time.

The FTC can do a lot of things, I think, to change practices in this field. I think, number one, it would be great to start a case -- a series of cases to establish that the SSN can’t be used as both an identifier and authenticator. It simply doesn't make sense. There are contexts in which you can use it as the same identification tool for both identity and for authentication, but the Social Security number is not one where that works.

I think it makes sense to promote competition among the CRAs, as I just noted. It definitely makes sense to start looking at fraud alerts and who's ignoring them, and there are actually companies that know who's ignoring those fraud alerts.

Look at a company like Debix. Debix is a company that will put a fraud alert on your consumer report and then you get this nice phone call to your cell phone and you're asked for a password. It's a spectacular program, this is not a product endorsement, but it's a way of putting more control in consumers' hands. Well, they know when those fraud alerts are ignored because credit is granted and the Debix system isn't triggered. So, companies like that offer a window into who's following good practices and who's not.

I do think it makes sense to revisit the red flags a year from now to see what is effective and not effective. And let me close just by saying, not to end on a negative note, but there is a lot of confusion still in this workshop between the definitions of identification and authentication, and it is just absolutely critical that we clear that up and that we use those terms very precisely. Because we’re hearing certain people out there who are engaging in authentication using both words, it seems, interchangeably.

But the other issue is that I’ve never heard the word “authorization” in the last two days. That’s kind of an interesting idea. We heard that we're going to be authenticated more often, but when can we have authentication without identification which is what we're used to and it’s common in many different commercial contexts and when can we think about authorization and with less than full identity being transferred? I mean, some of the federated models of identity that Bob discussed might be one way of getting to that.

With that, let me sit down and we can move on to Fred. But thanks very much for holding this workshop, and I'm looking forward to working with you more to see what we can do to stem the tide of identity theft.

MS. RICHARDS: Thanks, Chris. Fred?

MR. CATE: Thank you very much. If it's all right, I'm just going to speak from right here.

MS. RICHARDS: Sure.

MR. CATE: I came with one set of notes and after the first panel this morning, I made another set and after Chris' stimulating presentation where, in fact, the other panelists are the only people who cannot, in fact, see what it is that he's put up on the board behind us -- which I don't know about you, Jim, but makes me a nervous wreck -- I now have another set of notes. But let me not give all 67 points I would like to give and instead focus on maybe several highlights.

First of all, I think it's a useful, just, moment to put a little bit of perspective around this. Remember, even though we're talking about Social Security numbers, first of all, we don't actually really care about Social Security numbers. The FTC's mission is not to protect Social Security numbers, it's to protect individuals, and Social Security numbers are one part of a much bigger set of threats that face individuals. And that's a very complicated picture caused by a huge explosion in data, the development of powerful networks and storage capacities and so forth.

The growth of distant national and international commerce, so that we want to be able to be served by businesses and government agencies and universities who we, in fact, may never see, so even the poorer forms of identification and authentication and verification that we already use in the offline world are even worse in those settings.

And, yet, at the same time, consumer expectations have continued to grow. We want faster and more efficient access and we’re frankly, as I think the prior panel demonstrated and Chris highlighted, we’re pretty intolerant of things that slow down that access. So, the quickest way I know to get the password taken off your laptop is to be traveling and have it not work, and then if you're high enough up in the hierarchy, you beat the table, and then, suddenly, that great protection that was put in by an important policy decision is taken away because the speed of commerce demands there be more rapid access.

So, in the context of this much bigger set of issues, and particularly post-9/11, the sort of growing interest in being able to identify people in settings frankly unrelated to commerce. So, you know, flying here yesterday, to get on the plane, to get in the building, for some reason they wanted to see my driver's license. They didn’t check it against a list, they couldn’t have cared less what was on it, it could have been fake, it would have made no difference whatsoever. But because I was clever enough to have laminated plastic in my wallet, I got in this building.

So, these types of multiple uses often of the very same limited documents, limited sets of data, limited tools for identification are really at the heart of the problem we're talking about.

Now, in the face of that problem, I would say, responding to the topic of this panel, focusing on the supply of data is the wrong place to focus. First of all, it is a hopeless place to focus so even if it is the right place to focus, we're doomed to failure. But it’s also, I would argue, not the best place to focus.

So, I don't mean it's unwise to suggest to people that they protect their own data, that we not print our Social Security numbers on our checks and so forth. But that, rather, that if our goal here is to make people better off, to make them more secure, and at the same time, allow them to live in the modern economy, to say we're going to shut down data is not going to do it and that is all too often the focus of many of the types of comments we hear at meetings like this, comments filed beforehand in the voluminous public record leading up to this meeting, and it's just not a workable approach. And, in fact, it's one of the I find disappointing things in the President’s Identity Theft Task Force report, is how focused it is on controlling the supply of data as if anyone has any idea how to do that.

The much better place, the much more useful place and, in fact, where I think most of the effective tools have been focused, are to focus on the use of data. And the President's Identity Theft Task Force noted this, let me quote, “It should be made harder to misuse consumer data," and then offered these two recommendations reflecting the depth of its thinking on the issue. We should "Hold workshops on authentication" and "develop a comprehensive record on private sector use of Social Security numbers."

Now, frankly, that's frightening that the Identity Theft Task Force, that that was as far as it could go in terms of saying what might we do to make the use of Social Security numbers less likely to lead to identity theft. Although I give the FTC enormous credit in that this two-day workshop, and the process that it reflects the culmination of, is obviously designed to reflect both of these missions from the Task Force and, hopefully, will help develop that record so that specific use-related strategies can be put on the table.

Now, we've talked extensively and certainly extensively this morning about types of use-related strategies that would be effective, and it would seem pointless now to just repeat all of those. But the point is to simply make it harder for somebody to exploit a Social Security number or, frankly, other data. I'm not just interested in Social Security numbers, to commit harmful acts, to commit identity theft, to commit financial fraud, to impersonate someone in accessing an airplane or a government building or whatever our concern of the moment might be.

Now, in a fair and just world, I would just stop there. I’ve said one thing that wouldn’t work, I've said a better place to focus, and that would seem to be the end of it. But Chris has inspired me to go on. So, let me say the thing I think we have to worry about and that we have to be extremely cognizant of in thinking about these data use restrictions is the problem of unintended consequences, which are vast, and especially as we have moved to an information dependent economy and an information dependent society, we run the risk of causing problems much greater than the one that we were targeting at the start.

So, for example, do we increase fraud if we make data harder to access that's needed to do data-based authentication? We heard the example this morning, the Bureau of Motor Vehicle records no longer being available for these uses. We run the risk of ignoring other benefits that come from having a more accessible set of data.

The convenience issue is one which leaps out at me here. And, again, at some point, we're clearly going to have to draw a line and say not everything can be as convenient as we want it to be, but there is a trade-off and, frankly, I'm not sure consumers are going to sit still for types of regulations on data use that interfere too greatly with convenience.

One of the things we've seen in other areas of data security is that well thought out solutions that are come up with usually by technologically oriented people, often end up creating bigger problems. So, we say you have to change your password every week or every month, thereby assuring that people write their passwords down because they can no longer remember them.

Ebay and Paypal, two of my very favorite companies, now follow an excellent procedure, which is they don't let you change your password to anything you've set it as before, thereby assuring you will never remember your password and you write it down.

Indiana is considering a state law right now that will require that every password used in a publicly funded agency would include letters, characters and numbers, thereby ensuring that you will not be able to remember your password.

Collectively, we've managed to make the password almost unusable through our well-intentioned efforts to drive it out of the ability of people to remember. Frankly, we see the same issue with Social Security numbers. Many of us, my guess is most of us in this room, remember or can remember or are capable of remembering our Social Security number.

I went to get my flu vaccine from my university, it’s a university provided benefit, it's taxable and, therefore, I have to provide a Social Security number. However, under state law, we're not allowed to use Social Security numbers for our employee ID numbers, so I had to provide an employee ID number. It’s a benefit provided that’s funded through our insurance plan. Our insurance company, of course, no longer can use Social Security numbers, so I had to provide my insurance number. So, there on one piece of paper, now the perfect vehicle for identity theft, is my name, my address, my employee ID number, my Social Security number, and my insurance number.

We've accomplished a lot there. We have greatly inconvenienced me, we've increased the price of obtaining this valuable service, and we've created a wonderful paper which, when it was stolen the next day, would be the wonderful gift to the identity thieves. These are the types of unintended consequences that I worry about.

Another is distracting people or institutions from more important problems. Again, security breach notices are a wonderful two-edged sword, but one thing they've done is they’ve focused a lot of us in this room and a lot of law firms and PR agencies on managing the notice process. I don't really know what they've done for security. It's interesting, in congressional hearings on this, no one's advocating that they’ve increased security. They've advocated that they have increased the embarrassment to the companies so that companies might then come back around and increase security.

This seems like something of an inefficient process to notify hundreds of millions of people that data that was stolen on a laptop or otherwise lost may or may not pose any risk to let them worry about it so that this will increase pressure on companies, which is then divided between PR agencies and actually doing something about it. Surely we could do better.

We heard mention this morning about other types of problems. Phishing is an issue which, frankly, worries me a great deal more than Social Security numbers, especially as we see it get better and more effective. So, we're going to build these tremendous protections into the system and then I'm going to give away my keys to the system because I'm going to be fooled by an e-mail message into providing that as a step for authentication.

The question of perspective is one which I think we really must not lose sight of because by focusing on Social Security numbers to the exclusion of the bigger issue, which is protecting individuals, we run the risk of compromising that bigger mission in the pursuit of the much smaller one.

Now, two final points, and again, this was echoed by this morning's panel and also by Chris, so I am really repeating that which wiser people have said. In thinking about ways of restricting, of making data harder to use in an illicit way, we need to be careful not to ignore simple steps. Again, I'm often struck at meetings like this where we discuss often very sophisticated tools and what ID Analytics is doing and these very extremely involved technologies and systems, which I am extremely supportive of, but then I go home and deal with businesses who are not doing the most basic things that we know.

It was just two years ago that one of the nation's three largest banks set its default password on every consumer account to the Social Security number. We don't need a Nobel prize to know that that was dumb, it was dumb two years ago, it's still dumb today, and I suspect that there are still major businesses doing things like that.

The pre-approved credit offers. Again, the data suggests that they are not in any way linked to identity theft. On the other hand, it's a little hard to think why it's a good thing to be mailing these to people, live checks being maybe a better example. On a weekly basis, I get from my credit card company an envelope that says "important information regarding your account." This, by the way, is a lie. I don't understand why it's not prosecuted as deceptive advertising. You open it and it contains three live checks for your credit account.

Really, do we need a commission, do we need a Presidential Task Force to tell us that's not a good idea? By the way, they didn't figure out that's not a good idea. But a lot of this -- the training of people is a critical issue and one which I think we've heard amply discussed. I enjoyed Stuart's story and particularly this morning when I complained to my bank about setting my default password to the Social Security number, the very helpful operator said, why don't you change it to mother's maiden name, that's much more secure. Is there anything we could add to that?

Finally -- see, one advantage of sitting here is I'm now one person removed from my moderator, so for her to stop me, she has to go through Chris.

MS. RICHARDS: Wrap it up.

MR. CATE: But I can feel the tension coming from this end of the table.

Finally, I think one thing we do need to be incredibly aware of and that is victims, victims of identity theft who for years, the one consistent story we have from all of our surveys, even if they tell us that identity theft is going down, they tell us that victims' experiences are still traumatic dealing with true identity theft, getting those cases resolved. I think we're going to see more and more of that. We hear about the bank account being cleared out and, sure enough, it was settled later, but what do you do at that moment?

We've all had the experience of traveling abroad or in another state or in California, which is another country, and finding that we can't use our credit card because these wonderful fraud protection tools have shut down our credit. So, this is, again, to go back to the general theme of needing perspective and balance, if our solutions are worse than our problems, we're not going to have made the people we should be concerned about protecting any better off. Thank you.

MS. RICHARDS: Thank you. Jim?

MR. LEWIS: How do I follow Chris and Fred? This is ridiculous, but I'm going to try. First, let me thank the FTC. I think these are very valuable sessions and I actually learn a lot, and yesterday, I was listening to the webcast. The best part for me was that you could hear the speakers before the panel, so that was -- but I love stuff like that.

The panels have been great. This panel's supposed to talk about recommendations and since I’m, I think, the last speaker, I'm going to try to inflame you, okay? So, stand by.

I started doing stuff like this in January of '96, so we're coming up on 11 years, and I say that only because when you hear me make fun of some ideas it's probably because I tried them. There are some things only the government can do and establishing your identity is one of those things. The Social Security number has become a de facto government service, right? It's the de facto national identifier. There is no viable near-term alternative. So, we are going to have to continue to use the Social Security number, we just need to think of ways to use it better.

Why is it so good? Because it links across domains, it links across organizations. It's easy to change one organization, right? So, I work at a place, CSIS, we could take off all of our Social Security numbers and give us a new identity number, but getting another place to accept that number would be very difficult. That's why the SSN is going to be here for a long time. Live with it.

The situation is that the government is now providing a new, free service. It's under-regulated and underfunded. That's where I would focus my efforts. Companies could offer you an inferior alternative, it would cost more, not work in as many places and not be interoperable, what a great deal, why wouldn't I accept it? No, you've got a free service that's good and a private sector service that may not be as good, at least not yet, that may change over time.

Now, I want you to do two things, two things that will help close this panel. The first thing I want you to do is I want you to reach out and touch the chair in front of you and say the following words, "Real ID, scary." Okay? Did we get that out of the system? We are going to have to do things that are different to improve identification in the U.S. Real ID is part of that. People don't like, I don't care.

MR. LEWIS: The second thing I want you to do now, and this is more important, I want you to look into my eyes, you are growing sleepy, you will do as I say. Regulate, regulate. See, I told you I'd inflame you.

The answer here to how to deal with the Social Security number since it's not going away, since we absolutely need it, since so many people depend on it, is to improve its regulation. A lot of the concern we're talking about today is the result of the uneven -- I'd originally written weak and then I crossed it out and put in uneven. The uneven privacy and PII protections that U.S. have, some places they’re good, some places they aren't, some companies do great, some companies don’t.

When you have an uneven environment like that, the result is people have concern, they’re worried, they’re afraid, and that's what drives a lot of this. Making the PII environment more even would help us. How can you do that?

There's also problems with the business model, I think, in the credit industry. We heard Fred talk about that. That may cure itself in the next year, but we have to think about these business problems and how do we get companies to behave differently.

There are ideological objections to improving regulation for these kinds of things and that's why I had you say "real ID." Improving identity is not going to lead to a police state. Improving identity management is not going to lead to a police state. So, it's something we need to do for business.

So, I think the use of the Social Security number has to be regulated, right? We have to allow its use, but we have to put conditions on that use. What are some of the conditions you might want to think about, and you all know these by heart. In fact, if you want to say them along with me, feel free.

Notice and disclosure of Social Security number. Why are you collecting my number? What are you going to do with it? Tell me.

Consent, opt in. I don't care that much. I mean, I worked for the government for years, I gave my Social Security number, plus my fingerprint, plus my kid's maiden name, ten thousand times, but ask me, I mean, you’re a company, do I have an opt in choice, can I decide to use it? If I decide to opt out and you decide not to offer me the service, that’s okay. But I would say opt in.

Provide an alternative identifier. Now, we saw this succeed with driver's licenses, right? Your driver's license used to have your Social Security number on it. Somebody figured out that was a bad idea to be flashing it all the time, although they never look at it with Fred. With mine, they touch the picture, I guess that made them feel better.

But you can come up with alternative numbers and you might want to think about how to do that, companies can do that.

Breach notification. I, too, like Fred, once doubted breach notification. In fact, a mere two months ago, I was giving a talk somewhere and I said it was like asteroid notification. What are you supposed to do when an asteroid is coming? It’s like, well, I'll put up my umbrella, I'm safe.

But it turns out -- these are all corporate lawyers, I had the three other corporate lawyers on the panel jump on me and trample me and say, no, the general counsel in the company worries about this a lot, it changes company behavior. That's one of the things I like about regulation, it changes companies' behavior, and breach notification does have that effect. It's indirect. There might be a more direct way, but it doesn't hurt and you need to think carefully about it. A lot of them aren’t done right. We over notify.

There’s other things you can do. Instead of sending me a dopey letter that I’m going to throw out unopened anyhow, suppose you had to publish something, suppose you had to notify government agencies. Notification doesn't have to mean consumer notification. It can mean notifying the regulatory agencies, notifying some other people.

Having to take out a full page ad in the newspaper, that would be a good deterrent.

Assignment of liability. Again, think back to the credit card industry, and somebody said, I think, on the previous panel about how PCI is a good model. PCI has done quite well in the credit card industry in improving security. A lot of what drove that, though, was the assignment of liability. You are only liable for $50 of the loss on your credit card. In point of fact, most credit card companies now eat that.

Suppose we extended that assignment of liability in these identity theft cases. Suppose the consumer was no longer liable or they were only liable for 50 bucks or some other nominal sum. I think companies would suddenly discover the benefits of improved PII management.

I say that because regulation creates incentives for change. You want to take a minimal approach, minimal is best. You want to emphasize transparency and accountability. You don't want to get into prescribing technologies or laying out 10,000 rules. But regulations that create transparency, that increase accountability, will change companies' behavior.

My own view, after doing stuff like this for 11 years, is the market is not going to deliver, all right? I confess with shame that in 1996 I wrote a line in a presidential report that was never published that we didn't have to worry about stuff like this because the market would take care of it. Guess what, I was wrong. The market's not going to take care of it. This is a new service and we need new rules.

MS. RICHARDS: Okay.

MR. LEWIS: Inflammatory enough, you want me to say a few other things?

MS. RICHARDS: Thank you, no.

All right, Fred, how do we increase security? How do we make it harder to exploit Social Security numbers and other data to commit fraud? I mean, you gave examples of kind of bad ways to do it, but what are some of the good practices?

MR. CATE: Well, first of all, let me say I think in many instances the best role of the government is to create disincentives for the bad practices. So, this sort of goes along with Jim's -- actually, I agree with virtually everything that Jim said. But one of the difficulties is if you enshrine in government regulation a particular behavior then when the entire world passes you by, that behavior is still there 10 years later, still being regulated.

So, for example, I would use law to, guess I would initially say, educate, but ultimately I'm perfectly comfortable with the idea of regulating, to prohibit the use of Social Security number for a password anywhere, a password that's set by an entity. Under any condition, just a blanket prohibition. If an entity sets your password to a Social Security number, we could just have the statutory damages and Chris could go out and collect it.

I'm working for you, Chris. I'm doing the best I can here.

I think recognizing that a Social Security number is often used in its best form as an identifier because it links someone with a data set and then you can use the data set to identify them so that anyone who relies on a Social Security number alone, you know, are you who you say you are, what's your Social Security number, okay, you know a number, you must be that person. Just like the security guards out front asking, do you have a driver's license, I would regulate that out of existence. It's not worth the money we're spending on it.

I think we have to be more careful about how that's regulated because then the questions are, what are the next steps, what else can you do in terms of data identification?

The question about whether to regulate the Social Security number in terms of its being used as an alternative identifier, I personally would not regulate on for the reasons I said earlier. And, actually, I thought on this issue Jim was on both sides of the issue, which makes you unusually agreeable, which is, on the one hand, the great value of the Social Security number is that it works across settings. But if we regulate how it is used and if we regulate who can use it in each setting, we run the risk of losing that ability.

So, again, the words "transparency" and "minimalist" I think are good words to apply here and I would echo these.

MS. RICHARDS: Let's talk, all three of you, for a moment, about incentives. Jim Davis talked about how the breach at his university kind of spurred action. Others talked about changing incentives or creating incentives, someone said kind of follow the money and make the person who gets the money the person who's liable and responsible.

Can you talk about certain incentives that we can either put in place or change in order to help with this problem?

MR. HOOFNAGLE: Well, let me just start by saying that I'm in accord with Jim Lewis on the security breach notification issues. We actually just released a paper at Berkeley discussing the effects of security breach notification laws in which we interviewed chief information security officers, and they told us that having to give notice is such an embarrassing thing that they changed practices and that they were more powerful within their organizations, they could do things like establish audit measures, access controls and encryption. Encryption is the big one. They couldn't do it before those laws passed.

And, in fact, our paper cites to your colleague, Fred, of Hunton and Williams, who said that prior to the passage of these laws, she was recommending that companies not use encryption, it’s not worth it. So, there are a lot of ways to organize incentives, and the security breach notification law is one way to do it.

I should also mention that I'm quite fond of the law because my boss, Deirdre Mulligan, wrote it and, so, we're quite invested in it and it's not perfect. I actually think that there should be a risk trigger and most of the consumer community, I think, disagrees with that.

When you talk to companies about what privacy means to them they often say it means trust. And what that boils down to is the idea that they have to maintain a very good reputation, their customers have to feel warm and confident in their practices. But it's not any single thing. It's not necessarily complying with the law. But having to write a letter to your consumers, to your customers saying, we've lost your data, I'm sorry and you're going to have to do something about it, maybe run to high ground, the meteor's coming, right, it does affect the idea of trust and it does motivate organizations to do much more on security than they used to be doing and that's documented in detail in our paper.

MR. CATE: Can I just ask you in response to that, would that be any different if you just had to notify the attorney general and publish it in the press rather than -- in other words, certainly my experience, you know, a university with 100,000 people, we tend to mail a fair number of these notices, we have never gotten a call back on a single one. So, when you talk about that critical trust relationship; however, we also live in a state in which we have to notify the attorney general. That's the one that gets attention. So, it costs a lot less, but, of course, that's made public, it's posted on a website. The reputational harm is great and that's our primary regulator.

MR. HOOFNAGLE: In fact, one of the things we explain in the paper is the idea that if there were a publicly available database of security breaches, people could learn from each other’s breaches.

MR. CATE: Right.

MR. HOOFNAGLE: They can have that that could have been an us moment and say, we’re running the same type of server, let’s patch it up. So, I agree with you, Fred, about that. But I would say that I've been thinking about this, I don't know an area of American law where we say, we’re going to take away someone's rights because they don't use them. There's a rich study into the idea of why people don't do something when they have a legal right to take an action. So, yeah, there's a lot of consumers who are getting these letters and just tossing them.   But I can't think of how American law recognizes that practice and then says, okay, well, if a lot of people aren't using the rights, maybe none of them should have this right.

MR. CATE: But, Chris, that's a stretch, right, because we're not talking about taking away the right, we’re talking about taking away the individual notice. So, for example, I accrue rights every day. Every time I walk down the street, I accrue a right. There's a crack in the sidewalk, my ankle twists, we don't pay someone to stand there to hand me a notice to say the State's liable to you and here's your notice. The right remains unrelated to the notice.

I think the question here is what's the best way for consumers to be engaged in protecting their own security, if you will, their own privacy, their own financial identity?

And, here, I guess I go back to where Jim started which is, frankly, this is a problem that only the government's going to solve. And one of the sort of major reasons we are still dealing with this problem is that the government has failed to solve it. It has so largely deferred, so it said we're going to tighten the requirements for the states to issue driver's licenses, maybe, you know, in six years, if we get over the hump of states that resist to this and, by the way, it's not going to be a very valuable form, a very rigorous form of identification. But, by the way, we're going to make everyone photocopy that driver's license who’s a financial institution and keep it on the record, they just shifted the downward problem. It was a problem at the central level, now we'll make it a problem at the local level.

Getting our hands around this, so this is, I think, with breach notice is one of the issues. We're just shifting the problem. And, in reality, this is a problem only the government in the long run is going to deal with.

I, as you know, have argued much -- well, occasionally I find friends in the oddest places -- that we should just publish Social Security numbers, that would be the best incentive because then you would know they are not secret, they are not passwords. We've been publishing them for years. The IRS put them on your mailing labels for ages. And once they were published, then it would be clear, it would be negligence in the clearest state. We wouldn't hardly need additional regulation to say if you use a Social Security number as a password, you are being idiotic and here's a gun and you can just shoot yourself, rather than engage in lots of detailed regulation.

Then the Social Security number would actually serve that purpose we intend it to serve, across domains, and it would not be able to be used in any of these inappropriate ways we’ve talked about.

MR. HOOFNAGLE: Let me ask you a question in response to that. When you say SSN as a password, do you mean as a credit authenticator or as a password when I'm on whatever website? So, when you use the word “password” there, do you mean it broadly --

MR. CATE: I mean a password.

MR. HOOFNAGLE: Broadly as an authenticator or as --

MR. CATE: By itself as a authenticator, as a password. So, if I call up and say, hi, it’s Fred Cate, and they say, what's your Social Security number and I give it to them, and they say, great, we know it's you, I would call that a password use. If they say, great, now we can pull your file and now we’ve got some questions for you, that strikes me as a much more appropriate use of a Social Security number.

And, by the way, it doesn't matter that it be secret. If I give somebody else's Social Security number and they pull the file, I can't answer the questions.

MR. LEWIS: The last word, I think, on the incentive question is the word “liability.” So, you have to assign liability, assign it to the right people, assign it to the people who cause the problem, a lot of your issues will go away. So, identify those folks. I have some suspicions, it's not the consumer assigned liability.

MS. RICHARDS: Bob Sullivan yesterday said that people should have the right to see everything associated with them and their Social Security number in order to be able to correct information. What do you think of that idea?

MR. HOOFHNAGLE: There's a privacy tension in that idea because you might get information about other people in that inquiry. But going back to the recommendation that we should be moving from credit monitoring to identity scoring, I think kind of addresses what he's talking about. So, this is the idea that I might request my credit report, and because someone else is using my Social Security number but a different name and a date of birth, I might not see that information on my report.

And if we were to move towards identity scoring, as Ms. Litan at Gardner, has advocated, we might be able to shine a light on those and without getting credit report information about other people. Does that make any sense?

MR. CATE: Yeah, I mean, I would agree with that. I would say as a general matter -- let me say this, I think we need to be clear here about the difference between transparency and bureaucracy, and I think we've tended to move toward bureaucracy in this country. So, we inundate people with notices they don't read, they can’t understand and that don’t offer them any meaningful choices, and the idea of doing more of that strikes me as a bad idea. So, I would certainly not favor that, you know, a mandatory notice rule, although it would be very good for the lawyers in the room.

The idea of transparency, that you have rights to access certain data that’s relevant to decisions made about you strikes me as very sensible and then, as Chris has wisely pointed out, the difficult issue is how to make that work in an environment where you are authenticating people so you're not giving one person's data to somebody else.

MR. LEWIS: And the word you want to add to the transparency word is the accountability word. There is transparency, I think transparency's good. I see something, what do I do about it? And if it's not clear what I could do about it or if it's a long, complicated process, I really don't have any rights. So, you want to make my rights better, you know, expand the accountability.

MS. RICHARDS: The last question I have and then we'll open it up to the floor is to discuss a little bit the training and education and kind of the people in the room are not the ones who need to be trained and educated, and this is both the consumer and also businesses and how best we go about that.

MR. HOOFNAGLE: There's a great value in consumer education. I think that one of the problems here is the fraud -- the different types of attacks move so quickly, especially in the phishing area. As Fred pointed out, there are incredibly sophisticated phishing attacks, some of them are now relying upon social network connections. So, you appear to get an e-mail from your friend or maybe from someone of the opposite sex that you're attracted to and they're saying, you know, come to this website and share your information. There’s a great study, I believe, at Indiana on this very point.

So, education has a place in here, but it doesn't solve all the problems. And I wouldn't go so far as to say that we should be telling consumers to freeze their credit reports. I think that is a step that is not right for a lot of people. It's right for some, but not all. But it would make sense to have the fraud alert standard, I think, in all credit granting transactions. It's actually kind of shocking that until you invoke a fraud alert, there is no statutory risk-based standard for credit granting. It's only the point where you enable a fraud alert that you actually get language in the FCRA that says that the lender has to take reasonable steps to verify your identity. It seems like reasonable steps to verify an identity should be in place by default.

MR. LEWIS: I'm not a big fan of education and training, especially for consumers because, you know, you're never -- what's the take-up rate going to be? It's not going to be 100 percent. People are busy, they're not going to get to it.

I bought my mom a laptop for her birthday, it's her first like real computer. It's very funny talking to her on the phone, and I know there's a lot of people like that out there. So, education, great, swell, but don't expect a lot.

If you want people to pay attention, assign a penalty if they don't do something, then they'll learn, right? But if it's just sort of education out in a vacuum and training, you're not going to get that much for it. So, if you want to do education, fine, but then ask yourself, now that I've -- and you could even think of it as a trigger, you've been educated, you do something wrong, what happens to you then?

MR. CATE: It's so hard for someone in a university to hear education be -- of course, it's true, but it's still hard. It’s cruel, Jim, cruel.

I do believe in education. I think, in this case, education needs to be sort of targeted in different ways. So, one thing that I think matters a lot is having specific deliverable messages that we try to get people to focus on as opposed to getting them to understand the concept and the theory involved.

And I think here about fire safety. We've been sending fire safety questionnaires home with fourth graders for years now nationwide, where you go, do you have paint cans in the garage, yes or no? And, of course, these very simple questions, which you then bring back which have no consequence whatsoever, but prompt discussions that I'm sure lead to better behavior in homes.

Similarly, I think we all recognize that although industry catches a huge amount of fraud, for industry to catch all fraud, they're also going to catch more and more legitimate use and, suddenly, my credit card is going to be useless. So, we don't want to completely move away from a system in which people check their own credit card statements, people check their own checking account statements, people get their free credit report that Congress has allowed them to get on an annual basis. As far as I can tell virtually nobody does, these three basic things.

So, there are specific messages that we could educate to get even a 20 percent increase in, I think, would be helpful. But the place where I would focus education is on company employees, so that the people on the phone aren't doing the things that Stuart related this morning, aren't doing the things like I discussed with the bank. These are well-meaning people and they have many, many other things I know that companies are concerned about, efficiency and accuracy and accountability and Sarbanes-Oxley and all these other things. But, frankly, one of the things that it seems like they could use a fair amount more training in are basic privacy and security standards

MR. LEWIS: Let me pick up on that a little bit, and I know you want to get to questions, but I don't worry about companies figuring out best practices because they're smart, energetic and they'll do it, right? But I don't think we need to tell them here are the best practices, I don't think that's what Fred was implying. I think we need to tell them if you don't adopt best practices there will be penalties. And then they will have an incentive, and this gets back to the incentive and the cost thing. Give companies an incentive to provide the kind of training that Fred is talking about. Without that, it's going to be hard to get them to move.

MS. RICHARDS: Okay, so, I will get a microphone around to you. We'll start in the back there.

MR. KLOUDA: Thanks, Tom Klouda from the Senate Finance Committee. It's been a great session and a great panel today, and I've learned a lot. One thing, I was always very skeptical of breach notification approaches before this. It's helpful to hear that maybe, you know, not directly to consumers, but maybe to the AG, maybe something published in the paper would be great.

I guess I'm also wondering, you know, recently we've had a change with the hospitals where they're going to have to start reporting data on outcomes and health statistics. Has anybody proposed like requiring financial institutions, insurance companies and utilities to publish data on incidence of fraud loss or identity theft that has occurred from their organizations? I guess I'm sort of thinking that, in some ways, they've become the enablers of identity theft from the practices that we've heard discussed today, and if that information was published, as you said, that would sort of have a deterrent effect or a clean up your act effect. Thank you.

MR. CATE: I think that's right. Let me just offer one qualification, which I'm sure has already occurred to you, and that is on the whole, industry eats, in terms of individual consumers, the vast majority of losses due to fraud. Unlike a hospital, if a hospital cuts off my wrong foot, they can't do anything to spread that cost to make that better, whereas if my credit card is used fraudulently, my credit card company, by law, is going to make me whole to within $50 and by custom is going to make me whole to start with.

So, one thing we’d have to think about in reporting this and, frankly, I think many people have argued that we ought to have better reporting on fraud losses because, frankly, we have inadequate data available to regulators and, I would argue, to researchers, but is in ways of categorizing what those losses would be and how to make the reporting be useful as opposed to sort of aggregating everything together into a number that might not be useful.

MR. HOOFNAGLE: I have two quick responses to that. First, I filed a Freedom of Information Act request last year to get all the data that went to the FDIC and the other banking agencies as a result of the security standards notification law. So, basically, what I wanted was a spreadsheet that the agencies were maintaining detailing all the banks' security incidents.

Now, when we got the spreadsheet from FDIC, it was pretty terrible. It was difficult to determine if the spreadsheet even had a primary key. So, we couldn't tell how many incidents there were. And if you looked at the raw data, it looked as though there had been 1,200 incidents in the time period for which we had data. But we went back to the agency and we got a primary key and we found that there were about 400 incidents reported to the FDIC from their regulated banks, that they had to report under Gramm-Leach-Bliley. But we found that the reporting was incredibly uneven and almost completely useless, and this is going to come out in a report next week being issued by Gartner and there’s literally just a paragraph of the report, because the data are so bad.

Now, on the other hand, what I've done is I've proposed, in an article that came out yesterday, that credit lenders do publicly report how many incidents they have, the raw number of incidents of identity theft they have, how many they've avoided through fraud measures, how much they've lost, and the vector for fraud. Because I don't think we have good enough statistics, especially in light of the growth of or the advent of synthetic identify fraud and especially because at least one of the companies out there that’s studying identity theft has a lot of incentives to characterize the identity theft problem in a certain way.

And, so, to say that identity fraud is going down based on a poll, on a poll of victims inherently loses the synthetic problem for the most part, and I don't think we can truly say that the convenience check problem has gone down in incidents or the pre-screened offer problem. We keep on seeing anecdotal evidence of these offers being issued with very little authentication. I mean, one of the best examples I write about in my paper is the dog that got the credit card who worked at the Pupperoni factory.

MR. LEWIS: Just two quick points. If there's no harm, why do we report? And I agree, the data's terrible, you don’t get it. But if there’s no harm, maybe we don't need to report. And I say that because, in a political context, there might be a universe of things we want to do, that would not be my first priority of things I want to fix. So, you know, nice to have, not number one.

MR. OSCHERWITZ: Tom Oscherwitz with ID Analytics. First, a comment about what Chris said about reporting --

MS. RICHARDS: Hold your mic, thank you.

MR. OSCHERWITZ: Better now?

MS. RICHARDS: Yes.

MR. OSCHERWITZ: The first thought is, and I'm still working through this, is what would the incentives be for private sector organizations if they had to report and is it possible that it might actually create a deterrent to investigating more in fraud solutions because you actually might discover the fraud and then you’d have to report it because you're being proactive? So, that's a point.

But the other issue, I want to really focus on Social Security numbers and I think it's important to really focus on where we're at today. We live in the era of the Internet where information is widely available, SSNs are pervasive, and one thing to think about data breach notification laws is that most data breach notifications are breaches involving Social Security numbers that are reported on.

So, what we're saying here is we have a society where literally hundreds of millions of people have lost their SSNs or hundreds of millions of SSNs have been lost. So, the question is, when we're thinking about SSN policy, whether it's restrictions on use or trying to put the genie back in the box or it’s about how you use it going forward, I think we need to think about the fact that it's so far out there that it's already being lost hundreds of millions of times.

MR. HOOFNAGLE: I'll just be very quick. I think any time you have statistical reporting, there are some people who are going to play the numbers. I was flying back from JFK to SFO a couple weeks ago and I noticed that my return flight was seven hours and seven minutes long. I don't think the country has grown, I think that my airline perhaps said that the trip would be longer than it probably would be so they wouldn't be late. And, so, yes, I think there is a chance for bad incentives, but they can be overcome. And I think roughly it gets harder and harder to engage in playing the numbers when you have to tell a regulator about your internal safeguards, et cetera, under Sarbanes-Oxley and under Gramm-Leach-Bliley.

As far as the issue of so many SSNs being lost, I'm a believer in privacy law in some contexts where we've had Gramm-Leach-Bliley, for instance, laws that tried to put the genie back into the bottle and I do think that SSNs are less publicly available on certain sites because of Gramm-Leach-Bliley. It's not as easy to just go online and buy a Social Security number as it was six or seven years ago.

I think there's other examples out there. I think what's also interesting is that many of the people who said that the genie is out of the bottle have lobbied to get that genie out of that bottle, and we should think about that incentive.

But, you know, I love the Federal Trade Commission, I’ve been here many times working on many different issues, and I don't want to say they fooled you once story, but we’ve heard this over and over. We heard this about telemarketing, impossible to tackle, remember? Couldn't tackle it, too big of a problem. We tackled it. We should have some confidence in the track record for solving problems here.

MS. RICHARDS: Okay, we'll go to the gentleman.

MR. RIDINGS: Thank you for taking my question. I'm David Ridings with Namesake. I’m an attorney out of Tennessee, and I liked the court case that you alluded to a few moments ago.

I was wondering -- and I just want to say I know there’s a lot of very intelligent people in this room, there’s a lot of very powerful people in this room, and I welcome more of these type of panel discussions and would come to any of them that you have.

But this problem is so vast, there's so many ways to have your identity stolen and so many ways to be victimized that it's difficult to come up with an answer. Some of the answers are already in place, not being used properly. We've alluded to the credit fraud alert that's not being utilized properly in some cases. Many times they're not actually calling the number. That is something that I think we could legislate and create liability for ignoring that fraud alert.

I think that we could empower the consumers by enabling them to set the credit freezes themselves without it costing an enormous amount of money and to unset them. To set them when they're not going to be shopping and to unset them when they're out shopping for a house or a car. Things like that could empower the people to stop the new credit fraud cases. But the existing ones, I think moving away from the Social Security number as an authenticator and possibly going to biometrics, is that not something that we would be better suited to spend our money on than the billions of dollars every year that we're spending on identity theft?

And it's just a comment and maybe a rhetorical question, but thank you again for your time.

MS. RICHARDS: And I'll ask the panel that because that's kind of the issue of technology and advances there, biometrics and the mobile devices. Do you all want to talk at all about that, how technology might help solve this problem?

MR. LEWIS: Well, I'll start by saying that I used to collect authentication technologies and it was kind of like the Smithsonian approach because none of them actually worked. That's the problem with this. Eventually we will solve this, eventually we will get to someplace where there will be some way, better way to authenticate people. But, right now, there's a set of fundamental problems. The initial government documents, including the SSN, need to be improved. One of the benefits of things like Real ID and some of the other laws is we have better government processes for core identifiers.

This is a digital environment, so you say biometrics, cool, here's my thumbprint. In some cases, I translate the thumbprint into digits and then the digits go out over a computer. Guess what, I can copy those digits. I can do it. So, there is no perfect solution yet.

I'm a great believer in technological progress and perhaps, who knows, in the coming years, we'll see it. That's why I think for now we have to deal with the environment we're in and look for rules that will change the incentives for companies to do a better job of protecting this stuff.

MR. CATE: I would echo that and say biometrics may clearly be part of solutions in certain environments, but by no means is a silver bullet and, frankly, I don't see any technology that’s a silver bullet here. It underscores the point that this is such a broad issue.

It's funny, for example, to analogize it to telemarketing, I would say they have nothing in common. Telemarketing a child could have solved, it took political will. And the Commission and the states deserve enormous credit for having had that will to do it. This is a much bigger set, much more complicated, it goes to the core of the economy and how it works, and this is not going to be easy or solved by some particular bright idea.

Even the point that Tom made on reporting, I think it raises this question, no longer should we be seeing fraud as a company-by-company problem. It is much broader. Frankly, increasingly now, we ought to know the different experience because we're watching fraudsters move from company to company with synthetic identities that may be identified only by having multi-company data.

And, again, this is where we have conflicting issues. If our privacy laws lead us to crack down on the availability of this data for research, for analytical, for regulatory purposes, we may be missing the very thing we need to be getting at the breadth of this issue.

MR. HOOFNAGLE: I think consumers broadly would favor that multi-company data to detect fraud. But it's important to note that often security and authentication in these fields are stalking horses for other uses of data.

I’ve worked on SSN bills for a long time and they're almost always written in such a way that there is some marketing or other type of use that consumers could object strongly to, whereas they very much would want their SSN used for anti-fraud purposes. So, that stalking horse is out there and it takes a lot of discipline to see it and to deal with it.

MR. ROSE: I'm going to move up to the front here. I’m not just going to be talking to the panel but the whole bunch. It's been a great two and a half days, a very good job by the FTC and all the speakers.

I am Jim Rose. I am an associate in Protect ID. There's three of us involved, Bob Brooks and Craig Burkhardt.

What I have done actually is develop a system to solve a number of these problems. So, I’ve been kind of anxious to get up here and share this with you and let you mull it over and see what you think. I'll try and make it as brief as I can.

I spent quite a few years as a financial crimes investigator for the City of Duluth in Minnesota. So, if you have any trouble with my language, I'll call the interpreter up because I know we Minnesotans speak a little different.

Anyway, what started this for me is I come from a different perspective here. I created a system that was going to protect the consumer, first and foremost. I ended up with, oh, about a 70-year-old victim who was very frustrated with the process, got some information that the people using her ID were using the local Kmart, she actually staked it out and caught them. But the biggest problem she had was getting it fixed. She could not get her credit cleaned up. Three years later, she's coming back, still having problems.

That's what my incentive was. I needed to create a system, I felt, that would allow the consumer to cut the damage off at a point where they could recover more quickly. The end result of that was devising a system that would allow the individual consumer to pick a four-digit PIN number that is changeable on a 24-hour basis. So, if you think you're a victim, become a victim, you change your PIN, and that stops the use of all your other identity.

How does that solve some of the other problems? And I'll try and keep it short because I know that --

MS. RICHARDS: Please.

MR. ROSE: So, what happens is it would allow the SSNs to continued to be used exactly the way they are today with no changes at all because it is not a relevant number by itself any more. It only becomes an identifier, not an authenticator any more. The authenticator will be the four-digit PIN.

And as you start to expand and what is the incentive, because loss to retail will go down, they will get their money back. Because there's incentive. This program can be run as a for-profit business on a nationwide basis, there is an incentive to put it in.

MS. RICHARDS: I -- okay.

MR. ROSE: I'll be done in just a second. I'd be more than happy to sit and go over with anybody that's interested. We have some documents available. That is only a very small aspect of what happened here. It basically will deal with almost all of the problems that we've discussed in the last day and a half.

And it's been very nice to finally have this opportunity to come forward and let it be known that there is a very useable solution out there. Thank you.

MS. RICHARDS: Thank you.

MR. BLAKLEY: So, three things really quickly, two pieces of information and an argument.

The first is with respect to reporting fraud associated losses, Chris, you may want to go back with another request. Financial institutions have a regulatory obligation to maintain and report three years of audited historical data regarding operational risk associated losses under the Bael 2 Accord. Operational risk associated losses include losses due to failures of security.

So, it may be that there is another set of data that you could ask for that would be -- and, by the way, there is some evidence that this is changing behavior because of what you do if you report those losses, and they are acceptably small, is if you're a financial institution, you can significantly reduce the capital set-aside that you have to maintain to demonstrate financial integrity. So, you can put a lot more money into circulation and work for you if you can demonstrate that your losses are low.

There's some evidence that that is improving behavior, but it’s also a source of data that you might look for if you want to get more information.

MS. RICHARDS: I'm sorry, can you also identify yourself?

MR. BLAKLEY: I'm sorry, Bob Blakley from the Burton Group, which actually is relevant to my next point.

Chris, I want to depress you a little bit. You talked about a one-on-one relationship with credit reporting agencies. When we have been going around socializing this idea of the identity oracle -- I'm going to try to avoid embarrassing anybody in particular here by saying that we have spoken to very senior executives at more than one credit reporting agency about exactly going into the business that you propose and those executives successfully contained any hint of enthusiasm for the idea.

That's not that they said that it’s a bad idea, they simply listened politely and reacted as if they would if they had been inhabitants of Madame Tussaud's wax museum.

Last, with respect to Real ID, I just can't leave this one go. So, the competition for worst federal government idea in this decade is fierce and Real ID didn't win that one but it was in the finals. Starting from the false premise that we could prevent terrorism with stronger ID cards proceeding to then decide that because we had zero identification authorities, we should then move to 51-plus, and then choosing those 51 plus as the state Departments of Motor Vehicles and then giving that crack team of experts zero additional funding to complete the task, just doesn't seem like the way to solve the problem.

If we want a strong identity mandated by the federal government, the federal government should require us all to get passports and they should fund the State Department to actually implement that idea, and if necessary, for the purpose, raise our taxes. But Real ID is just a terrible way, at every level, to go about this problem.

MR. LEWIS: Well, I couldn't disagree more, and I think the story for Real ID is that the Motor Vehicle Administrators Association of America, and it includes Canada, too, were coming up with a set of rules on how you improve the process of getting a driver's license.

One of the things I used to do for fun when I was in the authentication business was make my own Utah state driver's licenses. There were 11 different ones. You could just pick any one you want. Setting rules, making people verify stuff, moving to harder-to-counterfeit driver's license? These are all good ideas.

When MVAA was doing it, when it was the state associations, no one complained, no one said it was an unfunded mandate. Congress hijacked the idea. Made it a little more kludgy, I agree with you, and now we heard all this complaint. But we have to start moving towards better credentials and I think Real ID is a step. So, we disagree. It's not popular, but it's a start.

MR. BLAKLEY: I agree on better credentials, I just hate the particular program.

MS. RICHARDS: All right, we've got about 20 or 25 minutes more, and then I'm going to have a couple of final answers. So, I just want to ask everyone, again, to kind of think about -- those of you who have been here for the last day and a half, this is kind of an opportunity for recommendations and, so, I encourage you to let us know what those are.

MR. SABBATH: Hi, I’m Larry Sabbath. I represent private investigators, and I just had to make one response to the last panel's discussion of how investigators might get access to the data they need for a lot of purposes and I think it just wasn't a real-world example.

The suggestion was that law enforcement’s exemption in most of the pending legislation could simply delegate that authority to private investigators. They just don't do that. I mean, it's hard enough to get the FBI to share information with local law enforcement. I think we're all familiar with that.

I think the reason you need private investigators and others who are capable of solving fraud and other crimes is simply because police authorities don't have the resources or the ability to do it. We heard yesterday from an Assistant U.S. Attorney who used to have a position here in Washington say that in Los Angeles the threshold for doing ID theft, I think, was 750,000. Even if it was 150, that's pretty darn high.

We have people in the audience here today who have been investigating mortgage fraud. There are more mortgage fraud investigations done by the people in this audience than were done last year by the public authorities. You cannot ask law enforcement to do all these jobs.

The Federal Trade Commission does a heck of a job. They've been asking for more money since I worked on the Hill and I left in 1989. They don't have the resources, they're not likely to get it from this administration or the next one. So, you need to have the ability to conduct these operations.

Secondly, the issue is not just identify fraud, but there's also other kinds of fraud. I think you have to understand that public police authorities, as a rule, are very good at looking at violent crimes. They're not very good at resolving fraud. They just don't have the ability, and in many cases, the jurisdictional ability, to do that, let alone the manpower. And I think if you ask them privately they will all admit that.

The General Accounting Office has found that to be the case specifically with regard to identity fraud.

Secondly, we're not just talking about the criminal kinds of work that private investigators do --

MS. RICHARDS: Sir, what's -- I'm sorry, do you have a recommendation for us for --

MR. SABBATH: I do have recommendations, but what I'm responding to was the suggestion that the recommendations on the Hill would work and, in fact, they won't, and I'm suggesting there needs to be an opportunity for investigators and others who have a valid reason for the information to receive it.

What I think we should do are three things: One is you should not display private information on documents. That's largely being done in many instances. But I think we need to pick off the low-hanging fruit.

Secondly, I don't think that private information should be sold on the Internet to anybody who's got $25 and a keyboard, and I think the private investigation community would agree to that.

Third, I think that credit granters ought to be required to authenticate with more than a Social Security card. What I'm suggesting is that the broad brush solution that says we're not going to allow Social Security numbers to be sold to anyone and that we’re going to list three or four exceptions and hope that we're not creating all sorts of unintended consequences can't ever work. That's my suggestion.

MR. HOOFNAGLE: Larry, you make several excellent points. Let me say that I work with a private investigator to do some of the work at Berkeley and in my former job and I have a lot of respect for private investigators and they're definitely necessary in the scheme work of law enforcement.

The tensions that are here, and this is actually recommendations that I think should be considered. I'm sorry for not putting them on the slide.

But one of them is universal licensure. Private investigators are not licensed in all states, and in states where they are not licensed, there are a lot of people performing activities that would normally fall in the framework of what a licensed investigator would do. So, on one hand, you have no licensure. In some states, you have pro forma licensure.

The other kind of tension here from a privacy perspective is that creating access to Social Security number or other similar information based on your status is always viewed with skepticism. So, you look at like the Drivers' Privacy Protect Act has an exemption in it that allows private investigators to get access to drivers’ data for an enumerated purpose under the Act. You don't get the data because you're a PI, you get the data because you're a PI plus you are engaging in one of these 13 approved behaviors. And, so, those are some of the issues that are creating tension here.

I'll mention that yesterday I talked about the indictment against investigators in Washington. Five of them, according to the indictment, were licensed investigators and two of them were working for those five licensed investigators. We have a general accountability problem here, and for someone who's worked on the Amy Boyer case, this is not just identity theft, it's stalking and some very dangerous stuff going on. The Amy Boyer case involved a licensed investigator who was basically allowing someone to practice under his license illegally.

I think, clearly, one recommendation that should flow is to have national requirements for licensure and some type of framework of enforcement similar to what you have for lawyers.

MS. RICHARDS: Go ahead, you've got the microphone.

DR. ANTON: Annie Anton, North Carolina State University and ThePrivacyPlace.

I'd like to echo what Mr. Hoofnagle said when he said that we need more confidence in what we can do. We've put a man on the moon, we have engineered unmanned air vehicles, we have engineered vehicles that can cross the desert in California, and this is not that complex of a problem. The problem is that we need the incentives.

As a computer scientist who works very closely in the area of regulatory compliance and software systems, I can tell you that the thing that limits our ability to create technical solutions the most is all of the exceptions in every single law governing the use, collection and exchange of information. And if we were to provide an environment in which scientists and technologists can work in an unfettered process to try to create a solution for this, without consideration of the law, we could solve this problem very quickly, I believe.

And, so, I don't know how we solve that problem, I don't know how we set up incentives that would enable us to create those kinds of solutions that could then be adopted and maybe the laws could be revisited because then we can tweak the software in some way.

And, secondly, I wanted to respond to Mr. Cate that is it really that bad to write your passwords out on a piece of paper. We solved the problem of how to secure a piece of paper a long, long-time ago. And there are lots of software solutions to help you encrypt all of your passwords. I know that I have over 80 passwords. I don't know the account names or the passwords for most of the things that I do because I encrypt it all or I have it securely written somewhere that no one else can find it.

And, so, I think that just saying that because we can't remember something it's not a good password is not quite accurate. Thank you.

MR. CATE: Let me just say in response to the last point, I think it highlights the gulf between computer people and the rest of us, because the rest of us aren't using our computers just sitting at a desk with an encryption program that's running software to manage our 80 passwords. We're using them every day as we travel, as we move around, as we use our cell phones, as we try to obtain service via an 800 number when a flight is cancelled. That's exactly the problem. In other words, I certainly agree it is much easier to build solutions if you work from an office and those solutions work in that environment only.

The problem is we're dealing now with a ubiquitous information environment and I think the problem is actually quite complex. I do echo, though, what I took to be the research point, and certainly I hear this often from researchers both at IU and elsewhere, it is very difficult to do certain types of research in this area because of running the risk of running afoul of illegal protections yourself. I'm not remotely suggesting we abandon those legal protections to facilitate that research, but it is something that lawmakers and law enforcers might be thinking about as to -- really going back to Chris’ point about if we license private investigators, do we have any way of facilitating research in an environment that would be useful here without subjecting researchers to criminal liability for their behavior.

MS. GIVENS: Two suggestions for research --

MS. RICHARDS: I’m sorry, could you restate your name?

MS. GIVENS: Beth Givens, Privacy Rights Clearinghouse. We’re a consumer advocacy organization.

Yesterday, Lael from Home Depot said a freeze is not the answer, quote, unquote, and today Chris, Chris said it's not right for all. Actually, I agree with you, Chris. But freezes, I think, are an answer for aggressive identity thieves. By the way, in case you don't know what a freeze is when you freeze your credit report, it basically cuts off access to it so if a thief goes to Circuit City to buy a large screen television and says, oh, by the way, I want to open up an instant credit account, Circuit City cannot get access to a credit report and, hopefully, they have enough sense to not then issue instant credit.

I think it's very effective, but we really don't know. So, my suggestion would be research on the effectiveness of freezes, and also in that research study, take a look at the various fees that are being assessed across the states. I know Consumers Union said it should be no more than $5. I agree with that, but what effect do the fees have as a barrier to people signing up for the security freeze.

And then just, secondly, James, I believe you said if there's no harm, then why should there be reporting? This is number two, not related to security freezes. If there’s no harm, why should there be all this reporting? And I would say we really don't know.

Fred, you know my response to what you said, on the same response, the Javelin Survey says that only 30 percent of the victims know their perpetrator. The Javelin Study also says only 40 percent know how it happened. So, we really don't know if a breach does or does not result in harm. I would recommend getting -- maybe finding actual victims, drilling down and doing some one-on-one survey questioning with them, maybe by an anthropologist or a communications scholar, and learn as much as you can from victims so that we can do a better job than just say, hey, if there's no harm, why do we need to report? We don't know.

MR. LEWIS: Well, I don't think we want to overload the canoe here on regulations. So, I wouldn't put that kind of reporting at the top of the list.

On the freeze idea, make it easier for people to do, and when Home Depot or whoever, and I don't mean to pick on them, of course, sells that television based on fraudulent information, make them bear the price. A lot of the problem will go away if you do those two things.

But reporting, I hear this from the FBI all the time, the banks won't talk to them. How much is it worth pushing on this one when there are other areas we could push on and make some progress?

MR. HOOFNAGLE: Let me just mention on freeze. In 2003, I wrote an article where I actually argued that files should be frozen by default. I have since changed my mind about that. The reason why is what freeze is about is really kind of a vote of no confidence in the authentication system. And I think if we could find ways to give incentives to improve that authentication system, we wouldn't need freezes except for those terrible cases where you have really persistent imposters.

So, with that, the fact that all these states have passed laws saying we're just going to take these people out of the credit market and they're going to have to go through this process and pay money in order to buy that big screen television at Best Buy or whatever, that is a huge vote of no confidence in the current system. And I think it, in itself, should be driving some serious reform.

MR. MESSIS: Good afternoon and thank you very much for the panel. My name is Jimmy Messis and I'm the Editor-In-Chief of Professional Investigator Magazine.

I'd like to focus on the recommendations because I think that's what this section is all about. Being here for the last day and a half, I've heard that maybe millions of people have access to Social Security numbers. So, the problem is not the access, the problem is the authentication process.

Let's assume that it's out there, that everybody does have it. We deal with, as investigators, with the victims and I haven't heard any victims speak here, so I'm a little disappointed. But perhaps I can speak on behalf of some of the ones that we've worked for. Most of the victims became victims because the financial institutions gave credit cards out without doing any authentication or it was done by a computer. When we did the investigation, we found that it should have never happened in the first place.

But here's my other concern: Where did the victims have to go? When they go to the local police department and let's say the person who stole their identity was from another state, the local police say, all right, I’ll take your report, thank you very much and good-bye. Then the person calls the credit card company and the credit card company -- the person says, my identity has been stolen and the response is usually, oh, really, are you sure, well, we're going to have to prove that you really are the victim of identity theft. So, now, they're the victim again.

My concern is, why didn't the bank check the identity of the first person in the first place and that could have prevented it?

So, one of the words that I heard here yesterday and today was multi-step authentication, multi-factoring authentication. I just recently did a cross-country trip, and as I'm using my credit card in the gas station, I had to put in my ZIP code for the billing address. It was a step. Many financial institutions have not instituted any steps. So that person can go right to the Circuit City, get instant credit and walk away with a big screen TV.

So, my recommendation, not from an investigator, but from a consumer, is there has to be more authentication levels and the SS number is certainly not one of them. Thank you.

MS. RICHARDS: And I would note that there is information for victims including a universal police report and other information. So, we have moved to try to make it easier for victims once they have been -- both to deter and also to defend once someone has been subject to identity theft.

MR. McCARTNEY: Jim McCartney, Bearing Point. A couple things on recommendations; first, no matter what we do, we're wrong. Somebody's going to disagree, somebody's going to say you're not doing the right thing, and that includes doing nothing. So, the fact that somebody disagrees should not preclude us from acting.

I wanted to address training versus education. I think we need to stress education over training. Stuart, your example with the birth certificate was an example of training. She was taught what to do not why to do it. And you have to understand -- just to use an example, would you rather have your child get sex education or sex training? Sorry, it was a little crass, but, you know, that's a great way to look at it. I think we need to focus on the accuracy of the data.

And you talk about incentives, I think we need to have incentives on making sure that the data's accurate, both in the collection and in the transfer. And, so, there ought to be penalties for and liabilities associated with transferring inaccurate data and holding those people accountable.

There ought to be a correction process. The credit reporting agencies have a process. We ought to make sure there's processes in place for other organizations to be able to make that. But it ought to be somewhat painful. Correcting your credit report is not a painless event, you have to do a lot of work, that way it precludes or reduces the chance that people committing fraud won't be able to make those changes.

I like the idea of opting in rather than opting out. A lot of people don't like that particularly in marketing. The IRS tried to put out a rule last year that said if you want to -- for people collecting information on taxes, that they would have to make, in plain language, a notification of what they wanted to do and people clearly opt in. Well, that was decried, ironically from both sides. The privacy people said it wasn't far enough, the marketing people said it was too far.

Most importantly, I don't think we can rely on the federal government, and particularly the FTC, to do all the things that we want done. It's a great place to start and they can have some great influence, but it's got to go beyond that because as I said, number one, that’s not the role of the government, but, number two, we just don't have the money to put towards that.

MS. RICHARDS: Okay, I'm going to ask the panel a question. So, we've talked about creating a market for security, we've talked about authentication and prohibiting silly procedures, as someone said earlier. Perhaps using Social Security number alone to authenticate is not a reasonable procedure, but might be considered a silly procedure.

Retention, someone talked about, you know, we've solved the paper problem. Well, there were some regulations where you have to maintain paper for seven years in some cases. Do we need to prohibit the storage of SSNs when there's not a legitimate need for them? The internal identifier, how Social Security numbers not be used as the sole identifier. And training and education. Kind of how it's not so much the Social Security number in and of itself, but the linking and the increasingly linking these numbers to other data that is an issue.

And then synthetic identity theft and you have all the protections in the world, but if you're able to just take a name here and match it with someone else's number there and make up a third and fourth and fifth piece of information and also be able to get credit and other services, kind of, what can we do about that?

So, are there any things, are there any recommendations or thoughts that we haven't talked about yet that you want to raise, both things that the government can do currently and other things that need to be done by legislation? There was a lot of discussion earlier about regulating being the key.

So, if you all could let me know what further recommendation you make and what legislative change might need to be done. Chris?

MR. HOOFNAGLE: Sure. We had talked on the conference call about, you know, prior to this panel, you know, if we could change one law or one practice what would they be, and I thought a lot about that. I think if we had more reporting of fraud, we would be able to determine whether or not interventions work or not, whether the red flag guidelines are worth the millions of dollars you're spending to implement them.

But absent reporting, I do think that the default standard for credit granting should be the statutory legal standard and the FCRA when a consumer has a fraud alert in place. It seems to me, you know, the FCRA says that if you have a fraud alert in place, you have to use reasonable procedures to ensure that you are reasonably certain about the identity of the credit applicant. That seems like that should be the default standard. Anything less suggests that you could use unreasonable steps and be unreasonable in your credit granting.

If we could change one practice, I think it's pretty clear, and I think there's probably some accord on this panel, that the SSN be only used as a record locator and never as a authenticator.

MR. CATE: I agree, which puts me in an awkward situation. I'm not used to being in with Chris.

It seems that the critical issue is how the Social Security number is used and I would just reiterate this point. Focusing on where it is or how available is it or can we put the genie back in the bottle, if we lived in a perfect world with infinite resources might be a worthwhile thing to focus on. But the question is, how is it used and how can we make its use less likely to result in harm to individuals, businesses and the economy?

I think it will have to be done through a combination of regulation and liability, and that the hard issue is going to be getting that line right because the problem of liability alone is you can spend vast resources chasing around legal actions trying to find one that sticks, at which case, you know, we throw enormous damages typically against the unsuccessful defendant to send a signal to everybody else, and that doesn't seem like an overly rational way to approach this.

But in the absence of regulation to start moving us in that direction, that's going to be the inevitable way, and I think the Tennessee case Chris described points that out.

What we're looking at are really basic, straightforward regulations that would start the process of saying, what is the reasonable use of a Social Security number, and I think Chris' suggestion is an excellent place to start.

MR. LEWIS: It's difficult to think about regulation because the way we want to regulate might be changing a little bit. And, so, you have a larger problem that goes beyond the FTC about how do you regulate, how do you govern. Within the caveat, I think we all up here say we have to accept SSN use for some purposes, for most of the purposes it's used for now.

When I think about regulation, then, I would want to say avoid prescribing good behavior. So, we've had many suggestions don't let people do this, don't let people do that, that's not what I think is the best path to go down, because prescriptive remedies, although I love them personally, prescriptive remedies tend to fail, there's always some way around it or it doesn’t catch. So, you want regulations that deter and punish bad behavior, that means identifying what that bad behavior is. We accept that you can use it, but here are the instances where it's reasonably regarded as misuse; if you do that, you will be subject to some punishment.

The second thing is to think about regulation as an incentive and I usually think of it as a negative incentive. An incentive is I give you money to do something, well, the government isn't going to do that. But what I can do is I can do a negative incentive, which is, I'm going to take away money from you if you don't do something. So, how would you design regulations that create these negative incentives for companies? That's what you'd want to think about, negative incentives that get them to change their behavior.

Finally, I think about, you know, the liability issue that Fred brought up is a good one. Regulations need to think about who gets tagged, who is liable, who is accountable. So, we want to shift the cost to the entity that made the mistake. If a store lets someone buy an expensive television using my credit account, I did not make the mistake, they made the mistake, make them pay.

So, there's sort of three general rules -- four, I guess. You know, don't prescribe, think about how to punish and deter, create negative incentives, and then shift the cost to whoever it was that made the error. And with that, I'm happy with using the Social Security number.

MS. RICHARDS: Fred and Chris, are there other things that we should avoid doing? What's the one thing you don't want to come out of this?

MR. CATE: Well, the one thing I would say is I think we know today the vast majority of the fight against fraud is being fought by industry, and in many instances quite successfully. And, so, the worst possible thing we could do would be to create disincentives for the type of behavior that is currently, in many instances, winning the battle against some types of fraud. So, I think that would be a critical issue.

And then the second, which I would point to, which really I guess just reiterates what Jim said, but we almost always in law are fighting yesterday's problem. So, by the time we collect data and we come up with a consensus, we've got the perfect solution to the problem that is no longer really the pressing problem. So, it is critical that we not, through regulation or liability or through any measures, put in place systems that deter the ability of companies and individuals in the government and universities and whoever else to address the emerging problem.

So, if that's synthetic identity fraud, that would be a perfect example. Almost all of our tools so far have focused on fraud where there’s a real individual who can really go look up their credit report or really bring a complaint or really check their credit card statement. We need to be thinking in terms of incentives for solutions for emerging or changing trajectories of fraud, at the very least making sure we're not creating disincentives for those responses.

MR. HOOFNAGLE: It’s a difficult question. I think Jim and Fred both make excellent points here.

I would point out that it's all about incentives and the more prescriptive laws create bigger problems, I think, for the reasons that Fred mentioned. That's one of the reasons why I like the security breach notification law. It doesn't tell people how to engage in security generally.

We might also think about how other parts of consumer law create bad incentives for consumers. I think one example is the liability limits and the time in which you need to report fraud when you use your American Express card versus using Paypal. I never thought that that made sense, that you should have less protection in the latter. So, to consumers, they don't kind of distinguish between the products. In the advent of phishing, creating these types of incentives probably doesn't make a lot of sense.

The last area, I think, that we haven't visited and, I'm sorry, I just wrote it down so I remembered it, is we should think about tax policy. Companies that experience fraud write off the fraud losses. That is a serious pressure point for creating incentives, both negative and positive. You could just imagine the various approaches, which could include capping the amount that can be written off or, of course, based on market capitalization or number of accounts, that is complex stuff. But it could eat at the bottom line to an extent that it's not currently.

MS. RICHARDS: Okay, I think we have time for one more question or one more solution from the field. So, let's -- I don't think you've spoken yet. We'll do two.

MS. BOCRA: Thank you, my name is Nicole Bocra and I am a private investigator here in Virginia and up in New Jersey.

I do have two points and two recommendations, if you would. I like the fact that the panel has said going forward about the mitigating risk and to assign liability and to make people responsible for what's going on. I think, realistically, we have victims, which obviously care about what happens, and I believe the companies do care what happens to the people, their customers. The problem is there's a disconnect in that what do you do about it?

And one of my recommendations is, you're right, get rid of the tax fraud write-off, make sure they can't reduce their risks, and I think that's a great idea. The

IRS is going to love it, too.

But, realistically speaking, you need to make people responsible for what happens. It is that person that answers the phone that is well-trained and doesn't necessarily know why they're asking that question. Now, you can call countries and they're overseas and you can't even get someone that speaks English half the time, let alone understand what you’re asking. So, that's my one recommendation.

My second recommendation is that the FTC has done a fantastic job of consumer protection and they're not going to have enough money to go ahead and continue to educate everyone. So, you have to put the responsibility on to the businesses and on to the entities. So, I think from a personal standpoint, that's my recommendation.

From an investigative standpoint, I think Chris had mentioned about licensing throughout the states or nationally for private investigators, and I think that's going to be very difficult to do based on individual state laws. However, all of us are subject to individual licensing and registrations within our state. And I need everyone to keep in mind that I'm not a law enforcement officer, so if you get into a car accident and the police are investigating it, you can't hire me as a private investigator for your defense if I can't have access to the same record that they have. So, people need to think about that as well. That is why we're here on behalf of our associations. Thank you.

MS. BELLAMY: Hi, Lael Bellamy with Home Depot. I really appreciate the panel today. I think you guys have done a terrific job.

A little bit of what we talked about yesterday was trying to go after the bad guys and, certainly, there are bad actors in every industry and PIs, although I have a lot of respect for PIs and law enforcement, all of those people, certainly there are bad actors in every single one of those who are potentially going to misuse data for a variety of reasons.

Since we believe that identity theft is more than 50 percent insider issues, I guess what I'm really concerned about is really going after the bad guys. I don't think the bad guys are the retailers or the banks and I certainly believe that consumers need to be protected. But the example you used about the big screen TV, 99.9 percent of the time that's not the consumer's problem. That ends up being a fight between the bank and the retailer, and a lot of times neither one of them are necessarily at fault. It's the bad guy who comes in with the fantastic ID or the fake ID or the stolen sister's ID or whatever that is.

That's the problem that I would really like to figure out how to address is how to have -- if someone walks into my store with a gun and holds up people, they go to jail for a long period of time. If there's a little ring in a call center that does a bad thing or a rogue employee who does a bad thing, not as many bad things happen to the person, it's not the same thing. And some would say there's more damage inflicted on the people whose identities have been stolen.

So, to me, that's really where we should be focusing as well as on the real bad guys.

MR. HOOFNAGLE: One issue that we hadn't visited that I think you raised and Nicole raised in this two-day exercise is the issue of outsourcing and off shoring some of these functions and what that means for security of the Social Security number. It would be interesting to see how many institutions are transferring that information overseas, what the controls are, especially in light of some recent articles where reporters were able to buy full consumer records from call center employees.

MR. CATE: I think this last comment really is a good, if depressing, note on which to end because it highlights the complexity of this issue. And I think it also highlights the complexity of thinking of solutions because if you just take the question who's the bad guy, we know that a fair amount of consumer fraud originates from the actual legitimate consumer and we have ample evidence for this. I'm not talking about identity theft issues, I'm talking about I let somebody else use my credit card and then I don't want to pay for it, so I dispute the charge. We've got lots of congressional testimony from credit card companies about how many of the "I didn't make this charge" calls they get really do come from the responsible party.

In some instances, we have a clearly identified third party, if you will, bad guy. You know, the gun example, you could do the same thing with financial data. In some instances, I think we would say companies are the bad guys. In other words, the company that grants credit doing nothing to verify identity, doing nothing to match up the driver's license with the face, like the FTC security, that itself should appropriately, I would argue, take on a certain amount of liability.

The problem is all three situations are presented undoubtedly every day in every setting we're talking about. And what we don't want to do is get the incentives wrong or else we run the risk of conflating these very different situations and creating disincentives for what is currently better behavior going on.

MR. LEWIS: But I think we also see -- so, I see it as a positive note. We also see the kernel of a solution here. Fred and I were gossiping during Chris' slide presentation since we couldn't see it. When you get a passport, it doesn't look like a rigorous process upfront. Behind the scenes, a lot goes on. There's a lot of checking. One of the nice things about the Internet is you can automate and make that checking much faster.

What is it you do when you get a car rental? Well, they go through some sort of process here. They're not going to give you a car just on your smiley face. There is no instant credit in the car rental business. And, so, I think the emphasis here, the focus for me when you think about regulations is, how do we improve those back office procedures to make them more robust, to do a better job? And then you will have a much stronger case against that consumer who comes in and says -- and, sure, people are always going to game the system, I didn't make that charge. Right now, when it's uncertain, it's harder to fight. Make the back office better and a lot of these problems will start to go away.

MS. RICHARDS: I want to thank the audience and also the panelists here and turn the mic over to Joel Winston for closing remarks.

(Applause.)

CLOSING REMARKS

MR. WINSTON: I'm going to keep this very brief because I don't know about you but I'm hungry and it's lunchtime, so I'll keep this moving.

One of the measures of a good workshop is how many people stick around to the end, and we've really had a lot of people stick around to the end. So, I take that to be a good sign. I thought it was a terrific workshop. And I think we achieved the purpose, which was to really identify areas of consensus about this issue and solutions and areas that there's still some disagreement about, and I think there's a lot of consensus about a lot of issues.

I think there's widespread agreement that SSNs, at least today, are really the most effective way that's out there to match people with information, that is, for identification. There's really nothing else out there that's unique and permanent and as universally used as an SSN.

And we also talked a lot over the last day and a half about the legal requirements for using SSNs. So, for all those reasons, I think everyone would agree that SSNs are going to be around for a while.

I think there's also general acknowledgment, though, that identity theft remains a big problem. Stuart mentioned maybe some positive trends, that may be the case, but it's still a big problem. There are still millions of consumers each year whose identities are stolen. And even beyond that, consumers are frightened.

Survey after survey shows that consumers are very concerned about the integrity of the information about them, about which companies are maintaining, and they're very concerned about the consequences of identity theft. So, it's important for all of us to address that concern as best we can.

There's also, I think, general agreement about the role that SSNs play in identity theft. Some people refer to it as the keys to the kingdom. I think other people say that it may not be quite that important, but it's part of it. SSNs do play a role.

Thieves are getting more sophisticated, that's clearly the case. They're finding new and inventive ways of getting more information, limited only by their imaginations, and they're able to compile lots of information about people in ways that they never could before.

And then maybe, most importantly, I think there's a pretty widespread consensus that SSNs do not work well as a sole authenticator and that the problems arise when they're used both as identifiers and to authenticate. At the same time, I think there's widespread recognition that SSNs do play an important role in authentication, principally to provide access to third-party databases and other information that is then used in the authentication process. Fraud databases, for example, or a consumer reporting agency database.

Yet, there still seem to be some companies, we've heard at least some anecdotes over the last day and a half, that are authenticating people simply on the basis of a Social Security number or even the last four digits of an SSN, and I think we all agree that's really a bad idea.

As far as solutions are concerned, I think there were a lot of good ideas that came out in this last session as well as throughout the workshop. I think there's a recognition that these are complex issues, that's a word I often use, and I think it really applies in this situation. It's a difficult issue to resolve. There's a real risk of unintended consequences if we don't do it the right way. So, we need to be careful.

We realize there are a lot of trade-offs in some of these remedies and the most obvious one is if you make authentication too difficult consumers are going to fight back. You need to balance those two concerns.

We also have to address the fact that switching business systems is expensive, that's something that has to be taken into account as well.

Yet, I think there's still an uncertainty, at least in my mind, and I'll harken back to a question I asked earlier on in the workshop and that is, if there's still as many as perhaps three million new account frauds that are taking place every year, how is that happening if the authentication that financial institutions and other creditors are using are good? Where's the leakage in the system? Is it because they're not as good as people say they are or is it because that there are some bad actors out there? Of course, none of the people here today, as I think we’ve established that there's some bad actors out there somewhere who are not doing a good job with authentication.

Is it a training and education problem? We talked about that in the last panel and we certainly heard some anecdotes about the panelists who called up to get access to their account and were read back their name and address and Social Security number. Why is that happening?

So, I think we need to really kind of address that issue. Where is the leakage in the system and where can we best intervene to make it better?

I think there was a lot of agreement about the fact that this remains a problem or as long as this remains a problem, that we should all be working to discontinue or limit the uses of Social Security numbers where we don't need them. Putting them on ID cards, I think that was kind of a no-brainer that people talked about. So, that's something else I think people would agree to.

New technologies are going to play a role. Everyone agrees on that. Although it may not be the ultimate panacea. It's a moving target. I think there's a lot of discussion today about the different -- or the last day and a half about the different ways in which information is obtained and used and to put in place a single form of authentication and mandate it is probably a very bad idea.

So, where does the process go from here? Well, we're going to be taking this information and the other information we've gathered over the last several months and working with our partners in the other Task Force agencies, coming up with a series of recommendations to present to the President early next year. And we'll be publishing those. They will be public. And I think everything we've learned over the last day and a half is going to play a major role in doing that.

And then I want to just mention that I don't believe I've ever heard Fred Cate speak positively about government regulation but he sort of did today, although he kind of took it back later on. But most people agree that the government has a role to play here and I'm glad to hear it.

Thank you to everyone for coming. I really appreciate it. All the panelists were terrific. The people who provided breakfast, I really appreciated that personally and, of course, the FTC staff who put this together who are scattered throughout the room and worked long and hard hours to make this work as well as it did. So, thank you to everyone.

(Applause.)

(The workshop was concluded.)

CERTIFICATION OF REPORTER

MATTER NUMBER: P075414

CASE TITLE: SECURITY IN NUMBERS SSNS AND ID THEFT

DATE: DECEMBER 11, 2007

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: JANUARY 7, 2008

KAREN GUY

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

ELIZABETH M. FARRELL