FEDERAL TRADE COMMISSION

SECURITY IN NUMBERS

SSNS AND ID THEFT

Monday, December 10, 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

P R O C E E D I N G S

- - - - -

WELCOME AND INTRODUCTORY REMARKS

MS. COHEN: Good morning, everyone. Good morning and welcome to the Security in Numbers workshop. We're delighted to welcome you here today for what promises to be a dynamic and informative event.

Before we begin, we just have a few announcements. A few reminders about security. If you leave the building for lunch or at any other time, you have to be rescreened through security, so leave enough time to get back in.

Also, please wear your name tag at all times. And if you notice anything suspicious, report it to the guards.

You will see bios for the panelists in the folders that you got when you checked in, and there's information on local restaurants for lunch out at the materials table.

Also, please turn off your cell phones or set them to vibrate while you're in the conference area. And if you need to use your cell phone, please go out to the lobby or into the phone room to use them.

The restrooms are located across the lobby behind the elevators. I think there are signs set up to

point you in the right direction.

Fire exits are through the main doors at the front of the building on New Jersey Avenue and through the pantry area, which is straight back here, that takes you out to G street. In the event of emergency, please proceed to the building diagonally across Massachusetts Avenue.

The workshop is being webcast, and we are going to leave time for audience questions at the end of virtually every panel. So, because it's being webcast, please be sure to speak clearly into the microphone.

Also, the FTC is providing a free WiFi hot spot for anyone who wants to use that, and there are brochures on the materials table that give you the keyword to use that.

And, finally, I would like to thank ID Analytics for providing the breakfast and the coffee that's out front. Thank you very much, I know I enjoyed it.

Now, to welcome you here, I'd like to introduce Lydia Parnes, the Director of the Bureau of Consumer Protection here at the FTC.

(Applause.)

MS. PARNES: Thank you very much and thank you all for coming here on what is kind of a dark and dreary

Monday morning in December. We appreciate you all coming out to this workshop on private sector uses of Social Security numbers, a very important subject for us.

This workshop that we're conducting for the next two days is one of a series of steps that have been recommended by the President's Identity Theft Task Force to help reduce and possibly, perhaps, eliminate the circumstances that allow identity theft to threaten consumers' well-being.

The task before us is not an easy one and we understand that. Certainly Social Security numbers serve an important function. They're used by businesses to track and identify their customers and are an important fraud prevention tool as such. When used across businesses, they also serve as a single convenient key for consumers to use to unlock many important services.

We want to maintain these benefits while minimizing the ability of identity thieves to use Social Security numbers. Your presence here today, both in person and through our webcast, and your active participation in this issue is critical to helping us balance these interests.

Understanding the private sector use of Social Security numbers begins with a discussion of some of the traditional ways organizations have relied on the SSN. I

hope that you've all had a chance to take a look at our staff summary of information provided on private sector uses of SSNs released on November 30th. The summary details the private sector's uses of Social Security numbers in a broad variety of industries and contexts.

As the summary indicates, virtually every American citizen has a Social Security number. Originally enacted in 1935 to report employee earnings for purposes of the new Social Security program, the SSN's use has greatly expanded over the years. Now, organizations use the Social Security number to authenticate consumers' identities, keep track of them internally and identify them when requesting information from a third party. And these uses provide convenience and cost savings for both businesses and consumers.

For example, it certainly is convenient for consumers to have one identifier that lets them access bank, hospital, or insurance records. I know personally remembering a half dozen numbers -- remembering one number, actually, is hard enough for me. Companies can run an SSN through a third-party database of individuals known to have committed fraud to prevent possible fraudulent transactions. In this way, SSNs can be used to prevent fraud and consumer injury and also to keep costs down for businesses and, ultimately, for consumers.

In many cases, the current uses of the Social Security number have been driven by federal or state legal requirements. Businesses, for example, must collect employees' Social Security numbers for inclusion on tax forms required by the IRS.

The expanded use of SSNs in the consumer identification and authentication process, however, has a significant downside, the increased risk that criminals will use a Social Security number to steal a consumer's identity and obtain benefits in his or her name.

SSNs have been used for years by identity thieves to open new financial accounts and access existing accounts of unsuspecting victims, obtain medical benefits and secure employment. Identity theft associated with the Social Security number has profound individual impact, and those of you who have been involved in this area for some time I'm certain all have heard your own stories.

A recent complaint that we received really highlights this. It was from the mother of a boy with Down's Syndrome. She apparently learned that her son's identity had been stolen when his disability benefit statements, linked to his Social Security number, reported income from a company operating pubs in another state. She also received a call from a bank seeking to

collect thousands of dollars in credit card debt.

When she tried to obtain the credit file for her son, she was unable to do so. And it's likely because the thief had by then populated the file sufficiently to make it difficult for the true owner to prove ownership of the file. Ultimately, she was able to learn that the thief had obtained six credit cards and a car loan using her son's identity. As this example so vividly demonstrates, identity theft remains a serious concern with serious adverse individual effects.

Your comments, as reflected in our summary document, recognize that a number of organizations are taking steps to switch from their use of SSNs to alternate identifiers and to reduce their reliance on the Social Security number for authentication purposes. We applaud all of these efforts. We appreciate that there are often significant costs associated with these changes, but that they are an investment in a more secure system.

Notwithstanding these recent steps, consumers remain concerned about the seemingly ubiquitous collection of Social Security numbers by businesses. One recent survey found that 87 percent of consumers had been asked for either all or part of their Social Security number within the past year. Seventy-eight percent of

those surveyed indicated that they would prefer not to provide their Social Security number, but are concerned about their ability to obtain services if they fail to do so.

The fact that ID theft continues to exact a painful toll on a substantial number of consumers and businesses provides the context for this workshop and the backdrop for the principal questions we're here to answer.

How do the collection and use of Social Security numbers by the private sector contribute to the ongoing problem of identity theft? Are there specific steps we should take to address these concerns? How can we take such steps and retain the benefits of using Social Security numbers? And how can we do so in a cost-effective manner?

Our workshop will probe the dual role of SSNs as effective identifiers and as tools for identity thieves. The workshop, however, is just one component of the strategic plan developed by the Identity Theft Task Force to reduce identity theft. We've been very busy with other components of the strategic plan, and I just want to briefly highlight a few of the things that we've done already.

Although this workshop focuses on private

sector use of SSNs, we recognize that the federal government also must safeguard sensitive consumer data and minimize its unnecessary use, and the federal government certainly is a big user of Social Security numbers. So far, the Office of Personnel Management has issued guidance to federal agencies on the use of the SSN and is developing a new unique employee number to minimize reliance on the SSN for personnel uses in the federal system.

We're also reaching out to state and local governments to promote better data security and reduce their use and display of Social Security numbers.

As the Task Force recognized, the private sector must properly safeguard sensitive consumer information, including SSNs. So, the FTC and other Task Force agencies continue enforcement work in this area. Over the past few years, the FTC has brought 15 enforcement actions against businesses for their failure to provide reasonable data security, and we should be announcing additional cases in the very near future.

Education and outreach are also core elements of our campaign against identity theft. I'm sure you're all aware by now of our consumer education initiatives, including the absolutely fabulous OnGuard Online, which is designed to educate consumers about basic consumer

computer security.

We make sure to direct our education efforts to businesses as well. A few months ago, the FTC released a business guide on data security which has proven to be very popular, and just last week we released an online data security tutorial. If you haven't seen it yet, take a moment to check it out at ftc.gov/infosecurity.

Through the tutorial, users can learn about data security from business people in this very creative fictional small town. They share experiences, find answers to common questions about protecting personal information in their care. It's innovative, it's informative, and it actually showcases one of our own attorneys, who's not only a great lawyer but also a great actor.

We encourage businesses and associations to get involved by educating others. To that end, we'll hold two briefings here next week, on December 17th and December 20th, to describe the many educational resources that we are making available to support efforts by businesses to improve their data security. A poster summarizing the events and resources is right outside in the hallway, along with copies of our many publications. In addition, we have a flyer summarizing how to take advantage of these resources. It's included in your

conference materials.

Ultimately, preventing identity theft is about protecting consumers. And because of that, we're especially concerned about identity theft victims. The Department of Justice has revised its training for victim assistance counselors and the ABA is working with us and the Department to develop a pro bono network to assist identity theft victims. And every U.S. Attorney's Office now has an ID theft coordinator, an Assistant U.S. Attorney who serves as a point of contact to coordinate ID theft-related activities.

Many have forged stronger connections with state and local law enforcement to establish ID theft task forces. These groups promote better coordination and already have led to some meaningful prosecutions.

These are just a few of the other Task Force projects that are underway. But the work doesn't stop with the Task Force recommendations. As you all know, the FTC and the financial regulatory agencies recently released the final Red Flags Rule. These rules and accompanying guidelines require financial institutions and creditors to develop and implement an identity theft prevention program. The Red Flags Rules also mark a significant advancement in our overall strategy to attack and reduce identity thefts, and we're optimistic that the

rules will lead to substantial improvement in businesses' ability to detect and prevent identity theft from occurring.

So now, back to the workshop. Joel Winston is going to address in more detail how the workshop will proceed, what the panels will address, and where we hope to end up at the end of the workshop tomorrow afternoon.

Before I turn this panel over to Joel, I want to extend my thanks to the FTC's folks who put this workshop together. If you're here, raise your hand so we can acknowledge you. Pavneet Singh, Kristin Cohen, Christopher Olsen, Katherine Race Brin, and our paralegal, Marcy Baskin. And I'm not going to forget Betsy Broder, the Assistant Director in the Division of Privacy and Identity Protection, and Joel Winston, the Associate Director. They have both done a fabulous job in this area generally. It's not easy to put these workshops together and they've done a fantastic job.

I also want to thank all of the Task Force agencies for their help in putting this together and just for being terrific partners on this issue. Some of them are here today, are here this morning. Others will be here later in the day.

Finally, let me thank all of you in the audience for your participation in this important

discussion. I think the next two days will be really terrific. We expect a lot of hard work from everyone and some creative solutions. So thank you all and let me turn this over to Joel.

(Applause.)

INTRODUCTION TO WORKSHOP: FRAMING THE ISSUES

MR. WINSTON: Thank you, Lydia. Good morning, everyone. Let me be the second to welcome you and thank you for coming to today's workshop.

Over the next day and a half, you'll hear from an exceptional group of experts with diverse experiences and backgrounds from both the public and private sectors. They'll talk about the risks and benefits of the collection, use, and sharing of Social Security numbers in the private sector and they'll explore with you different ways to eliminate or limit the unnecessary usage of Social Security numbers.

As Lydia described, this workshop is about getting the balance right. Some observers have called for the elimination of the SSN as a means to identify or authenticate individuals. Others have argued that any restrictions on SSN use would be costly and ultimately harmful to consumers. Then there are those who have suggested, perhaps tongue in cheek, that the best solution would be to simply publish in a public forum everyone's Social Security number and thereby eliminate its value for identity thieves. These are people from the school of privacy, get over it.

These are all useful perspectives, or at least most of them are, and I don't want to prejudge, but my

guess is that the answer to this issue, how do you protect consumers from identity theft while allowing the benefits that flow from the use of Social Security numbers, lies somewhere in between. Again, it's finding the right balance.

I just noticed in today's USA Today, if there's any question about what the problem is here, the latest statistics on data theft. According to USA Today, the theft of personal data more than tripled this past year. More than 162 million records have been reported lost or stolen. And these entities that suffered these losses included 98 companies, 85 schools, 80 government agencies and 39 hospitals and clinics. Yet of all of these, arrests or prosecutions have been reported in just 19 cases. So, that gives you a sense of what the problem is.

In large part, SSN usage in the private sector has expanded because the SSN, which is a unique, permanent, and ubiquitous piece of information about individuals, is a convenient and cost-effective tool for identifying, matching and authenticating consumers. But, of course, it's that very usefulness of the SSN for legitimate purposes that makes it such a valuable tool for identity thieves.

In many situations, the SSN is a necessary, but

generally not sufficient, item of information that a criminal needs to steal an identity. For example, in most cases, a criminal cannot impersonate a consumer and open an account in the consumer's name without having that person's SSN.

So, to elaborate on some of the issues we want to hear about today, this is what we hope to learn more about. How do thieves get SSNs? How are they able to use them to open new accounts or to access existing accounts? What additional information do thieves need beyond an SSN? Are there substitutes for SSNs for identifying consumers that don't raise the same identity theft concerns? What would be the cost to corporations and other organizations if they had to switch to different identifiers?

More broadly, what would be the impact of generally restricting SSN use, disclosure, or display? To what extent are SSNs still used in the authentication process, that is, for verifying that an individual is who he or she claims to be? Are there better ways to authenticate consumers? And, ultimately, what can government do to help find the right balance on this issue?

Let me tell you a little bit more about the agenda for the next day and a half. Panel 1 this morning

will examine how thieves obtain SSNs and how they use them to commit identity theft. There are still many uncertainties about this linkage between SSNs and identity theft. Obviously, knowing how and the extent to which SSNs are used to steal identities is important when considering recommendations on what to do about the problem.

Our second panel will examine the private sector usage of SSNs as an internal identifier. That is, to match an individual with information about him within an organization. As I mentioned before, the SSN has clear advantages as an identifier, and, therefore, many organizations use the SSN as the employee or customer number or to track information about individuals. Some organizations, including some government agencies, even continue to print SSNs on an identification card making them easy prey for thieves, although far fewer do that now than did in the past.

It's good news, for example, that some universities have developed unique student numbers for display on identification cards while maintaining the SSNs in their databases for those people, like Lydia and myself, who are going to forget our identification numbers.

The panelists will discuss the ways in which

some private sector entities have moved away from using the SSN as an internal identifier and as an employee or customer number and the challenges and the costs of doing so.

The third panel will cover the widespread use of SSNs by organizations to link and share data with external entities. SSNs are used frequently to match individuals with databases that are used to help locate people, check credit histories, and provide background checks, among many other purposes. SSNs also allow healthcare providers to share medical information.

Again, proponents of SSN use argue that the SSN is uniquely suited for external matching purposes and that alternatives would be costly and less effective. Still, the widespread use of SSNs in cross organization information sharing carries the risk that the data will be compromised and misused. Participants on this third panel will discuss the costs and benefits of using the SSN to link data externally as well as possible alternative identifiers that might be less sensitive.

The fourth panel will address the use of SSNs for authentication purposes. Many private sector entities use SSNs in the process of verifying a customer's identity at the outset of a relationship, for example, when they open an account. Indeed, financial

institutions are generally required under the USA Patriot Act to collect certain information, including the SSN, when they open an account.

Many organizations also use the SSN for verification when granting consumers access to their existing accounts. One benefit of using the SSN for this purpose, as Lydia indicated, again is that the SSN is a number that most adults, at least, have committed to memory.

Many experts believe, however, that the SSN is not appropriate as the sole authenticator because it's so easily obtained and so commonly used. For that reason, the SSN often is used not just as an authenticator in its own right, but also to facilitate other forms of authentication. For example, many companies match identifying information provided in an application, including the SSN, with that found in third-party databases, such as that of consumer reporting agencies.

I think one of the key questions here is, how are thieves sometimes able to defeat the authentication requirements that businesses have for opening new accounts? Is it that the authentication measures aren't strong enough or are they inconsistently applied? Or is it that fraudsters have become more sophisticated and are able to compile richer sets of personal data about their

victims?

The fourth panel will explore these issues and the different ways in which organizations use SSNs in authentication.

The fifth panel will consider whether there are alternative ways of protecting consumers from identity theft without unduly restricting SSN use. They will discuss remedies such as improving authentication methodologies, enhancing customer controls of their credit records through tools, such as credit freezes, fraud alerts and credit monitoring, and using third-party identity providers, sometimes called identity oracles.

Finally, the mission of the sixth panel is a very broad one: Where do we go from here? This panel will reflect on all of the issues raised throughout the workshop and consider possible recommendations for the Task Force.

For example, should the private sector move away from using the SSN for identification and authentication, and if so, how? Or should we focus more on better protecting SSNs from misuse? Is there a role for legislation on this issue?

As you probably know, Congress has considered in recent years a number of bills that would more comprehensively restrict the collection, display,

purchase, sale or use of SSNs. To date, none of these bills have passed, of course. And there's a summary of recently proposed legislation in your information packets.

We hope many of you will ask questions, offer ideas and help us develop new solutions throughout the next day and a half. And, in particular, Panel 6 is designed to elicit as much audience participation as possible. So, plan to stay for the whole event if you can and we'll all benefit from your input.

Now, I'd like to kick off our first panel, which will address how SSNs are used to commit identity theft, introducing our moderator, Joan Meyer, of the Department of Justice. Joan is Senior Counsel to the Deputy Attorney General and she advises the DAG on policy and litigation matters involving identity theft, corporate fraud, procurement fraud, and healthcare fraud.

In addition, she manages the operation of the President's Corporate Fraud Task Force and she participated in the development and implementation of the Identity Theft Task Force. An impressive resume.

With that, I would like to invite Joan and our panelists for the first panel.

(Applause.)

PANEL 1: HOW SSNs ARE USED TO COMMIT ID THEFT

MS. MEYER: Good morning. As Joel noted, the first panel today is how Social Security numbers are used to commit identity theft, and we'll be talking about how thieves obtain Social Security numbers and how they use them.

We have a very distinguished group of panelists here today. First, we have John Webb. He's an Assistant United States Attorney from the Southern District of West Virginia. John is the Identity Theft Coordinator and Healthcare Fraud Coordinator for the district.

Previously, he was an AUSA in the Major Fraud Section of the United States Attorney's Office in the Central District of California in Los Angeles, where he served as Identity Theft Coordinator and prosecuted white collar fraud and economic crime. He also worked for the Social Security Administration. And he'll provide a prosecutorial view about how SSNs are used to commit identity theft and how they're obtained for such uses.

We also have Bob Sullivan on the telephone here today. He is a journalist for MSNBC. Bob writes about technology crime and consumer fraud. He is one of the nation's leading journalists covering identity fraud and he has written more than 100 articles on the subject. He also has a popular blog on MSNBC called "The Red Tape

Chronicles."

Bob will discuss recent surveys and studies regarding ID theft and identify any potential trends regarding SSNs' role in identity theft.

Then we have Lael Bellamy. Lael is the Legal Director of The Home Depot. She's responsible for all privacy, technology, telecom, outsourcing and e-commercing matters at the Home Depot. Earlier in her career, Lael worked at Choicepoint and she will discuss the extent to which SSNs are being used in ID theft in in-store instant credit contexts.

Then we have Chris Hoofnagle. Chris is a Senior Staff Attorney to the Samuelson Law, Technology and Public Policy Clinic and he's a Senior Fellow with the Berkeley Center for Law and Technology at U.C. Berkeley School of Law.

Chris is a nationally recognized expert in information privacy and he's testified before Congress and the California Senate and Assembly numerous times on SSN privacy and credit transactions. Chris will discuss trends in SSN use and its role in identity theft with an emphasis on synthetic identity theft.

The way this will work is that each of the panelists will give a 10-minute presentation. I'll ask them some questions, and then we'd like to open it up to

all of you to ask any questions that you like.

So, we'll start with John Webb.

MR. WEBB: Good morning, ladies and gentlemen. It's a pleasure and privilege to be here today to speak with you on a topic that has consumed so much of my time as a federal prosecutor for more than 10 years.

Identity theft and Social Security numbers go hand in hand. Identity theft and Social Security numbers are part of financial crimes, and Social Security numbers and the misuse of those numbers is a component of almost every financial crime.

Since the SSN plays such a pivotal role in identity theft, it’s not surprising that it's one of three personal identifiers that are most sought by identity thieves, the other two being names and birth certificates. The SSN provides a key access for identity thieves who their goal is to steal the financial benefits of the victim.

SSNs provide key access for identity thieves to be able to get to those benefits and misuse of the Social Security number occurs because the Social Security number is so critical to the proper functioning of our financial system. It's the most efficient and reliable way to match consumers to their credit and to other financial information. It's used as a breeder document for almost

all other false identification documents.

And most victims, ladies and gentlemen, don't know that their information has been stolen. Fifty-six percent of victims, according to FTC studies, don't know that their identities have been stolen until they're faced with some event that brings it to their attention.

The Social Security number is most often obtained illegally from the Internet or from street corners in large cities, such as street corners at MacArthur Park or Echo Park where any day, any time of the day or night, you can go and buy identity documents such as Social Security numbers, Social Security cards, driver's licenses and other documents.

Unfortunately, corrupt SSA employees have sometimes been the source of identity documents and false Social Security numbers by taking money for issuing those cards.

Counterfeit or altered cards are readily available most anywhere. As a matter of fact, if you have a printer, a laptop, and can get on the Internet, you can download the software that's necessary to print a Social Security card, and you can use that Social Security card for any number of reasons.

The theft of purses and wallets or the theft of mail is another source of obtaining Social Security cards

and other means of identification.

Some people have existing relationships with their victims, and as a result of that, steal from their victims. The neighbor down the street, the elderly lady who has a young person come and provide care-giving services, or just friends from the neighborhood that come into the home and steal identities.

And, of course, a significant means of obtaining identity, especially Social Security numbers, is in the workplace through your friends or people who you consider your friends or others that you work with.

Computers and the Internet are also the source of Social Security numbers and other means of identification. Now, you've heard the terms "phishing" and "hacking." They comprise approximately 1 percent of identity theft. How many of you have received e-mail asking you for personal information so that someone can send you a benefit in the mail? Maybe you've won the UK lottery. I don't know about you, but I think I'm probably the most lucky guy in the world because at least once a week, and usually several times a week, I receive notices that I've won the U.K., United Kingdom, lottery. And, unfortunately, I just haven't had time because I've been doing too many identity theft cases to collect that lottery prize.

Hacking is also a potential problem, individuals who have their computers taken over by another computer because of some website that you visited. Wallets and purses are also a large source of the theft of identity information and Social Security cards because when you have your car broken into because you're out jogging at a park and you don't want to carry your purse or your wallet with you, identity thieves know this. So, they'll break into your car and they'll steal your personal information.

And part of what you find in a wallet and your purses, checks, driver's license, credit cards, all of them identity documents and many of them providing direct access to your Social Security number.

Mail theft is a large problem, not only in rural areas but in large cities. For example, in West Virginia, we have problems with the theft of mail that is not a common problem in a place like Los Angeles. In West Virginia, people drive around the rural areas and they open mailboxes and they take out information such as utility bills, credit card statements, government checks and any other type of information that might be in the mailbox. And these identity thieves know the particular days that certain types of information is mailed. So, therefore, they know when to go to access that

information and to steal that information.

Now, pre-approved credit offers, those are a huge problem, ladies and gentlemen. That's why it's important to shred, shred, shred. Or, more importantly, get yourself off of those lists.

Tax information comes in the mail as well. Utility bills are a huge source of personal identifying information that are used by identity thieves and many of them still include your Social Security number on those bills. It is easy today to change your address by simply going online. It's convenient to you, when you want to do it, but it's also convenient for identity thieves when they want to do it. They can go online and divert your mail for a week, two weeks, a month, or permanently until they get the use of whatever it is in your mailbox that they want to get access to. And they can do that by going online and, suddenly, you don't get your utility bills or your credit card statement, and you won't know that.

Or maybe they only do it for a couple weeks and then the mail is diverted back and you don't even notice that you're missing a credit card statement or a utility bill. It's easy to do that online now. And also by telephone.

Dumpster diving, you've heard about that.

That's why, again, it's important to shred. Don't throw anything in your trash that you don't want someone else to see, including information that contains your Social Security number, as many pieces of personal information do.

How many of you have been solicited by telephone? Someone calls you up. They pretend to be someone they're not and they ask for your personal information. Elderly victims are targeted for this kind of solicitation. It happens all the time. It's very important that individuals don't provide their Social Security number or their bank account information.

Or someone calls you wanting to tell you that you've been solicited for jury duty and you didn't show up, you're in big trouble. But they can fix it for you. Just provide them with your personal information and they'll do it for you. There's all kinds of scams out there that request personal information.

Social engineering is a large problem. That can happen through someone pretending to be a landlord, an employer or a vendor. But workplace theft, ladies and gentlemen, is a very important problem to identity theft and a way or a means in which victims' Social Security numbers are lost.

Also, the DMV is sometimes a problem. Bank

tellers that ask you for your personal information or your Social Security number, when you go up to the teller line, if they ask you for that, ask for a piece of paper, write down your Social Security number and take that piece of paper back later. Don't let your number be spoken out loud in a teller line. That happens all the time with people skulking around banks for that purpose and for other means of attempting to take your personal information.

And, of course, skimming in restaurants, when you pay with your credit card.

Ladies and gentlemen, I'm out of time. Thank you very much. There's plenty of questions, I'm sure, later. Thank you.

MS. MEYER: Thank you very much, John.

And now we're going to turn it over to Bob Sullivan. He'll be participating by telephone.

MR. SULLIVAN: Can all of you hear me okay?

MS. MEYER: Yes.

MR. SULLIVAN: Oh, that's great, thank you. Well, first of all, I really want to apologize for not being there in person, but my identity was stolen and so I couldn't get on my plane. No. But I am going to be around tomorrow. So, if I say anything that really bothers you and would require a direct confrontation with

me, feel free to come up tomorrow and I'll say a quick hello to you.

Since I know it's hard in a room like that to listen over the phone, I'm going to keep my comments very, very brief. But there are just a couple of things I would like to bring out. Because this happened during the Thanksgiving week, I'll bet many of you didn't notice it, but there was a tremendous data leak over in the U.K. At the end of November, a government agency that sends checks out to families with children, all families with children, nearly half of the population, about 25 million people, it misplaced a couple of computer disks with personal information, including bank account information for nearly half of the U.K. population. Lots of folks are calling it the largest data disaster of our time certainly on a scale.

We've become a little bit numb to the millions and millions of numbers, but you can imagine if some government agency lost data on half of our population, what kind of reaction that would get.

And I bring that up for two reasons. One is despite the fact that we've been talking about this for a good four or five years now, you'd be hard-pressed to say that that situation is getting any better, that the leakage or theft of personal information is somehow

improving. I think it's pretty easy to make the case that things are getting worse and we should all be probably wondering why that is. But the other thing, and I'm going to circle back to this in a moment, is the theft of particularly sensitive information, bank account information.

So, this conference is about Social Security number use and display and collection. And when we were discussing what remarks we should all make, I found myself struggling mightily with the idea of limiting this discussion to SSN collection, and I realize, again, that's the focus of it and there's some legislation that directly addresses SSNs. But every time you talk about a data theft or identity theft all sorts of other pieces come into play. So, I'm going to apologize for stretching beyond SSN collection.

They wanted me to talk a little bit about recent studies, and so, I'll throw a couple of things at you. Everybody in the room I'm sure is familiar with Javelin and the work that it has done in identifying who criminals are and who victims are and who they are in relation to each other. And for some time we've had the idea, and Javelin research has suggested that roughly half the time in identity theft it's someone you know. So, it's a roommate or a family member, someone who has

physical access to you and they can thereby steal your wallet, maybe look at your records on your desk. But in some way or another, it's a person who is close to you.

There's new information on that front which doesn't necessarily dispute the Javelin numbers, but I think it might fill out the picture a little bit more. The Economic Crime Institute based at Utica College did a study over the past year or so, a very comprehensive study, where they looked at Secret Service prosecution files dating back to 2000, virtually every file. And what they found is that in all those federal cases only 8 percent of the time the victim knows the criminal. So a far, far smaller amount than we had thought, at least in that case.

Now, I think it needs to be said that the Utica study did not take a statistically significant sample of identity theft crimes, it was only federal cases that were prosecuted by the Secret Service. So, it's not necessarily representative of the entire national trend. But, on the other hand, I think it's really significant that in those cases not quite half the time, almost half the time, the data was actually stolen from some electronic means. So, you can say that there's a connection between collection of information, like Social Security numbers, and identity theft.

When it comes to SSN theft particularly, I always like to point out the problem of data collection at the time of employment. We do have a very significant problem of employees showing up and providing Social Security numbers when they get a job in our country and providing the wrong Social Security number. About nine to ten million times a year -- I'm sorry, nine to ten million people every year pay their taxes with the wrong Social Security number for all sorts of reasons, one of them being that they don't have a legitimate Social Security number to begin with, and as a result of that, there are millions of Americans walking around right now who are essentially lending or sharing their SSN with another person, and they have no way of knowing that and that's something that I think is incredibly important to address.

Because, fundamentally, I think that there's a genie out of the bottle problem here. If we were to restrict collection or display of Social Security numbers everywhere, it's hard to imagine that that would stop any determined identity thief because there's so many other ways to get it. I think it would be great to add some reason to the way that the system works today. But I think it would be even more powerful to give people the right to see everything there is to know about their own

Social Security number and to give them a chance to clean it up, because I think we all know that identity theft is almost inevitable and one of the most important things is giving people rights, once it happens, to find out about it and to do something about it.

But let me close with two points and then I'll pass it along. Now, Avivah Litan who's a very well-respected analyst in this field for Gartner, she did a quick report on the U.K. theft I mentioned earlier, the theft of -- I'm sorry, it wasn't a theft, it was the loss of half of the country's personal information. And she made the point that because it was banking information, it was a much more significant event than other losses that we've seen so far. And in her report she says that a stolen Social Security number, in some of those Internet chatrooms or where they're bartered, goes for about $5 or $10. Obviously, we all know that's a building block of information, but that sets a sort of market price to it, if you will. But a really hot banking account, a set of banking account information, can go for up to $400.

So that, I think, gives you some of the relative importance of these data points to be worth addressing all of these things together.

So, finally, as a journalist, I always have to

make this point. Again and again, we've heard from companies saying they don't just rely on the SSN to authenticate people now and that there's all sorts of back-end magic going on to keep people from doing things like opening up credit cards when all they have is someone else's SSN or their name or sometimes not even their name. But I'm here to tell you that I've done endless stories of people being able to get credit cards from companies, from big companies by doing things like using just a random SSN and a fake name.

One guy in California filled out a form and he used the name "Don't Waste Trees." He filled out one of those pre-approved credit card applications we just heard about, and sure enough, a few weeks later he got back an embossed card with the name "Don't Waste Trees" right on the card.

So, I wish that companies that were doing all of this to protect us would be a lot more transparent about what it is they're doing so that consumers could understand it and maybe feel a little better about the security of our SSNs, so that if inevitably we are forced to give it, we know that it really is being protected and we don't just have to trust someone telling us that and we also know what it is that we can do about it if something bad happens.

So, thank you again for your patience with listening to me over the phone, and I'll pass it along.

MS. MEYER: Thank you, Bob.

(Applause.)

MS. MEYER: Now we'll hear from Lael. Lael is the Legal Director at The Home Depot.

MS. BELLAMY: Hi, everybody. Thank you for having me. And many of my remarks today are not necessarily representative of Home Depot, it's my experience in the industry and talking to other people and all of that, so get that out of the way first.

It was really hard, this was a really hard topic because we're all very passionate about it and we want to balance the concerns about ID theft, which obviously harms consumers, but it harms businesses as well. And I don't think any of us, though, want to walk into a retail store and spend an hour in line because the poor person in front of us is having to remember who their mortgage is with and how much mortgage do they pay every month in order to authenticate a particular purchase going through the line.

And those are some of the proposals. A PIN number, other forms of identification that you could use in addition to the credit card. I'm not a big shopper, but I've been, of course, running around recently trying

to shop and I don't carry a lot of credit cards in my wallet, and I realized that I could walk in and then ask somebody to show my driver's license and then punch in my Social Security number typically on a PIN pad, and then get authorization to the account. So, that's really terrific for me as a consumer because I don't have to carry all of these cards and I can get more 10 percent offs and all those kind of things. It's very difficult -- it makes it harder to combat the identity theft that comes up as well.

Just a few things about what we've tried to do internally as a business first, and I can't talk about specific security measures and all that magic in the back room because I've been sworn to secrecy because we don't want to tell the bad guys about how we do protect information, but I can tell you that we certainly rely on more factors than just a credit card or just a Social Security number in order to get cards.

And I understand there's the Don't Waste Trees examples and all of those, but I actually personally tried to get a card online at Home Depot and typed in my business address because I guess I spend more time there than at home, and I got a little note back that said, oh, we'll be sending you a card shortly or sending you a note shortly about our decision.

So, I called our credit division, and I said, oh, I got this nice note. They said, Lael, that means that you didn't get the card, so you must have done something wrong. So, I realized they were authenticating it with my home address. And then I got a call and when I talked to the person on the phone, they made me run through several ways of matching up who I was. So, I think reputable companies have a number of measures in place to make sure that the right people are getting cards.

And the examples of the taped-back-together application or the "Don't Waste Trees" or whatever are maybe anecdotal as opposed to what everyone tries to do. Obviously, it's no benefit to us if it turns out it's the wrong person because then we just get the charge back. So, we are vested in making sure that the right people have the right information and, also, nobody wants consumers to be afraid to use their credit cards. Nobody wants consumers to be afraid to use the Internet because their identity's going to be stolen.

So, some of the things that we've done is we had a corporate-wide project that lasted almost two years where we tried to remove Social Security numbers from every place where we absolutely didn't need to use it. And it was a big fight with a lot of people who insisted

that they absolutely had to have the Social Security numbers. And, so, we tried to come up with ways to reduce those from our systems as much as we could, and then we also tried to come up with ways of replacing the number using employee identification numbers or other types of things.

We've also encrypted all of our laptops. We recently had our first encrypted laptop stolen, and I tell you, I've never seen so many people so happy about a laptop that was stolen, but we were like, woo hoo, now the bad guys can't do anything with it. So, we were very pleased there.

Another thing that I think a lot of people -- certainly the people in this room are aware of identity theft and I think there are certain groups and corporations who are more aware of it, for instance HR people or loss prevention/asset protection people, but unless you work for a bank or a credit bureau or something like that, I don't think that your average employee really thinks about identity theft that often, and that's really a sea change. Certainly, you worry about it if your identity has been stolen, but the difference between an employee who works for, say, Bank of America and an employee who works for a retailer, the focus is on customer service and helping the employee.

And, of course, you don't want to help anybody commit identity theft. But I do think it's very important to do things like this and to raise awareness.

One of the frustrations we have is -- that I personally have is I think there's too much focus on the electronic. Everybody's always worried about hackers and they're worried about the electronic databases. I think there's such a concern with paper, and one of my personal frustrations is we're required to keep the credit apps. Well, we take the credit apps and then we're required to send them to the credit card company. But then they're required to keep them for something like seven years, depending on what kind of record they think it is.

And that's so frustrating because now you've got a piece of paper that's got somebody's name and Social and address and all of that in there. And sometimes we see silly things, where a customer will fill out a credit app and then they won't give it to the person or give it to the customer service desk, they'll actually stick it back in the little place where they got the forms out of. They'll just fill it out and then they'll stick it back in there. So, I think again trying to raise people's awareness about what those are.

And, again, getting back to the balance between trying to help a consumer out who's had some type of

catastrophe or even just wants a new kitchen, you know, it's very difficult. Looking at the hurricanes, Hurricane Katrina, the fires out in California, we've had customers come in and have been unable to verify themselves, and trying to help those people go through this process, obtain credit to get tarps for their home or water or whatever it is out of the store that they need for basic health and safety and welfare, those are difficult things to try to do when someone actually can't verify themselves.

Another thing that we're seeing, too, which is kind of interesting, is there's not actually a consumer problem, we're seeing an issue with piggybacking, which is when people sort of loan their credit in order to loan their credit score to somebody else who piggybacks on their backs. The person who loans their credit never gets in trouble. The person who is riding on it will then run up enormous bills. We've seen this for millions and millions of dollars a month, especially in California, and then they leave the country or they end up sticking the retailer with most of those charges. So, that's very interesting to us and we would like to see those kind of things end.

One of the things that's very difficult, in my mind, is there's this sort of ever-present problem of

being able to prosecute the nickel-and-dime identity thefts because I think that's where a lot of these problems happen, and it's hard on the business and it's also hard on the consumer. It's particularly frustrating for the consumer when they can't get anybody to prosecute their particular case because of the small, potentially small dollar amount. And I understand certainly that there are problems with resources in all of this, but it's particularly frustrating, again and again you're being told, as a business, you've got to background check everybody, which we do. We require our vendors to background check everybody.

And then, unfortunately, these nickel-and-dime people who are getting together with small groups, whether they're in call centers or other types of places, collections, places where you're entering consumer or employee information, they take that information and use it to commit identity theft, and when they're caught they just quit and leave and they're never prosecuted. And it's extremely frustrating for all of us because you know somebody's done a bad thing and then, unfortunately, it's 5 or 10 or $15,000 and that really falls below the radar. So, because these people are never caught, they're never going to come back up on an employee background check.

So, that's certainly another thing that we're

particularly concerned about is -- and you see different figures, but I think it's about 50 percent are potentially from insiders.

We had a funny one I heard of recently. It turned out the girlfriend of a gang member had put herself into a collections department and was stealing people's credit card numbers and information. And then the business people were upset that the business didn't know that and, unfortunately, to my knowledge, or maybe fortunately if you're on the side of not wanting big brothers, there isn't a database out there of boyfriends and girlfriends and girlfriends of bad guys that you can use to try not to prosecute people or not employ certain people.

So, I'm getting my hook here. It is something that we take extremely seriously because we want people to have loyalty and trust in the system and in our brands, and we welcome any comments certainly that can help make the system better. Thank you.

(Applause.)

MS. MEYER: Chris.

MR. HOOFNAGLE: Good morning, everyone, and thanks very much for coming and for having me here. I wanted to thank the FTC staff for their very professional management in putting together and planning this

workshop. You know, the FTC in recent years has been tasked with an incredible amount of duties, reports to put out, enforcement actions to execute, et cetera, and they're doing a great job rising to the challenge. And I'd say one of the things we could do to deal with identity theft in this area, if anyone from the Hill is listening, is give more money to the FTC so they can continue their good work.

I'm also excited to be here because we're doing a lot of work in identity theft and security breaches at the Samuelson Clinic at U.C. Berkeley. My colleague, Jennifer Lynch, is here, who is our clinical fellow. She's actually written her law review article in identity theft, and I've been spending a lot of my time in this field as well.

Let me also take a moment to mention that one of our students just released a paper that's available on the Samuelson Clinic website about security breaches. And in this paper, she went out and actually interviewed chief information security officers and asked them about how security breaches have affected their practice. And it's really interesting. One of the main findings is that when companies learn about other security breaches they say, wait a minute, that could have happened to us. We're running this type of server, we're running this

type of authentication practice. Maybe we should take a look at our own practices.

So, I think that paper does shine a lot of light on uses of the Social Security number and how having more transparency of security breaches in a weird way can cause the prevention of other security breaches.

I'm also kind of excited to be here today because my paper on synthetic identity theft came out today and it's online at the Harvard Journal of Law and Technology. It's called, Identify Theft, Making the Unknown Knowns Known.

And with that, let me move along here. The basic hypothesis of this argument is that we rely so intensely on the Social Security number that it is, itself, becoming the basis for fraud. Some credit granters are authenticating credit applicants based on Social Security number alone and sometimes what they also do is look at the date of birth to see if the date of birth is keyed to the Social Security number. So, this has caused a problem of synthetic identity theft.

I'm not sure that we have a precise definition of this crime yet, but let me suggest it's a crime where someone uses a false name and information of another is one way of defining it. So, it's literally possible to take my Social Security number and my date of birth and

put your name on the application and get credit cards at some banks.

And the other implication of this is that if there isn't a name matching and if Social Security numbers are roughly tied to the date of birth and that's being used for authentication, the other implication is that you can just make up Social Security numbers, which is a real problem.

And I think some people ask, you know, why do you focus on this problem of synthetic identity theft? Well, I think it's that type of implication, that you can make up a Social Security number and still get a credit account, that actually shines a light on a lot of crimes that have more direct consumer harm. That is, if we can understand why this crime happens, I think we can understand better how to fight identity theft more generally. So, in a way, synthetic identity theft is an abstraction that we can use to help us think of other types of identity theft.

So, why is this possible? One of the main problems out there is that it's publicly known -- the link between the Social Security number and the date of birth is publicly known. And, so, I don't know if you can read that headline there but that's SSA.gov. So, that's the Social Security Administration, and it

publishes this chart every month showing the Social Security numbers that are tied to this month and year. So, you can see that if you generate a Social Security number based on these prefix and group numbers you can have a Social Security number that is matched to the date of birth sufficiently well to apply for credit in some contexts. So, this link is well-known. These charts are all over the place. Prior to them being online, they were in books. So, this information is very well known.

And, so, let me show you some articulations of this problem. This is an indictment in a case, U.S. versus Rose, in Arizona, a U.S. attorney has brought this case, a spectacular synthetic identity theft case. Rose and his friends are actually kind of sophisticated guys. They were retailers, they understood the consumer reporting agencies, they also had credit card machines to swipe cards. And they were actually creating identities and paying bills, et cetera, to create credit files on certain individuals that they could later bust out and steal a good amount of money.

But you can see what they were doing here is they were taking Social Security numbers that belonged to real people, attaching a fake name, sending the application to a drop box, so these cards from many different people would go to the same mailbox. And they

got 250 credit cards doing this scheme from 16 different banks.

So, we're not talking about -- remember, Bob Sullivan said there's a lot of magic going on behind the curtain. A lot of people will say, well, that's irresponsible retailers. These guys were able to hit up 15 different banks with this scheme and they're big banks. As you can see, Fleet is one of them.

I think the other interesting aspect of it is regarding the idea of nickel-and-dime thefts. If you look at this full indictment, all these counts, these accounts were only charged up to just under $5,000 and, so, the thieves obviously know that there's a certain limit at which banks don't investigate or that law enforcement won't become involved, and they did a whole lot of this before law enforcement got involved.

So, this raises an interesting point, and I hope I can talk about it a little bit tomorrow, and this is the idea that if we pass a privacy law it will reduce the ability to stop fraud efforts. This is really an example where very simple anti-fraud measures could have stopped these cards from being issued and privacy law would not have stepped in the way of simply doing name-matching to the SSN. I mean, we all know that there are private databases available that match name to SSN.

So, I think it's an important idea to view the argument that privacy law in this area will stop anti-fraud efforts with a little bit of skepticism because there are a lot of tools out there that aren't being used and that could be used to cut back on fraud.

And this is a great chart from ID Analytics. They have an incredible database that actually looks at applications across the network, across all sorts of different banks, and ID Analytics is going to talk later about their methods. But I really do think this is the way to look at the problem of identity theft and look at it more scientifically because they can look at applications and which ones were successful and which ones were not successful.

But when they looked at their database, literally of millions of applications, 88 percent of the events, 88 percent of the applications for new accounts didn't have a real name attached to the application, didn't have the correct name attached to the application.

And then the right-hand side there discusses the dollar losses from the type of false name fraud, and you can see it's quite successful in obtaining funds from banks.

I have a lot of questions about these charts. For instance, what exactly is the definition of synthetic

fraud that's used here? But if ID Analytics is right about this, there's a huge portion of identity theft out there that isn't readily observable by the various surveys that look at victims and actually call up victims and ask them, have you experienced this crime? So, I do think that this is the way to go in order to look more at this crime.

You know, I'm ahead of time here, so I'm just going to -- I'm going to do something refreshing, I've been outside of Washington for maybe too long. I'm just going to end it there and say thanks again for having me.

(Applause.)

MS. MEYER: Right now, we'll talk a little bit and ask some questions of the panelists. I'd first like to ask Chris, how big a problem is synthetic identity theft and how does it really affect consumers?

MR. HOOFNAGLE: Those are two very good questions. So, I think the size of the effective synthetic identity theft is known, the problem is we're asking the wrong people to determine its size. One of the proposals that I'm making in this article is the idea that financial institutions themselves should report on how much fraud they experience in any given year. They have to do that type of accounting in order to see whether or not they're profitable and in order to see

whether or not they comply with safety and soundness guidelines.

So, I'm not saying -- let me be very clear in saying that -- I'm saying that the FTC's identity fraud survey is great. And if any of you haven't read it, it just came out, you should look at it, it's a great tool. But it doesn't see the whole picture. And if we need to ask financial institutions to do greater reporting in this field, I think we could get a picture that would be more clearly in focus.

Does it harm consumers? That's another thing that -- there's a lot of argument on both sides. We see a lot of anecdotal reports of harm. Of course, the plural of anecdote is not data. So, we don't know for sure. But it seems to be reasonable to assume that if someone used my Social Security number and another name to get a credit card, the creditor is going to come after me at the end of the day. They're going to see that Social Security number, they're going to assume it's me. So, I would assume that it does affect consumers, but no one knows the extent to which it does.

MS. MEYER: Do you have any idea about how many synthetic identity theft prosecutions have been brought? I know you referenced that one in Arizona.

MR. HOOFNAGLE: I want to say that there's

another, but I don't -- I think there's only been two. The Rose case is very instructive in part because the indictment so clearly spells out the crime. But the other interesting thing about the Rose case is that you'll see that these cards were issued back in 2002 and 2003. So, it takes a long time for law enforcement to catch up. And these attacks change and, you know, synthetic identity theft is a problem that could be solved within a year and we could have a new problem out there.

MS. MEYER: Now, Chris had referenced, Lael, that we should require companies, institutions, to report instances of identity theft. What's your take on that?

MS. BELLAMY: I do think it's important for institutions to report identity theft. The thing I wrestle with is I think there's a definite over-notification issue, where, you know, a company loses tapes and they fall in the snow and, I mean, I'm thinking of an actual case where these tapes that only three servers in the world could run and they fell off the back of a truck and it was in the snow and the likelihood of harm is just so little. I think consumers are extremely alarmed when they get these notices and then, I think, if you get too many notices you just throw them all away and you don't respond to them at all.

So, I do think that there are two separate issues, when there's an actual loss or thought of real risk or real harm, I mean, I do agree, I think that that ought to be something that ought to be reported. I think it helps everybody. I like the idea that the chief information security officers are looking at what other people are doing, and we're particularly concerned about peer-to-peer sharing accidents and those kinds of things, that's been coming up recently as a potential issue. So, trying to balance that.

And then there's this other concern of identity thieves are apparently good at waiting, so they'll steal your stuff and then they'll sit on it for two or three years. So, if you're a business or somebody who's lost data, you know, it's hard to know, you might not know of any actual harm there, but maybe there is in the future and you might never know of that.

So, it's hard to have a crystal ball and see what's going to happen, but I like the idea. And I do think people should be authenticating on name and address and Social and all those things and I think that's going to become more important. I think more people are going to be doing that.

MS. MEYER: Now, I know that you, Lael, had referenced the problems with these identity thieves, and

Chris did, keeping the amount that they're stealing under $5,000. Could you talk, John, a little bit about the difficulties in putting together that kind of prosecution?

MR. WEBB: What Chris mentioned is a classic what we call credit card bust-out scheme, and you can't do that without creating the kind of documentation through the use of Social Security numbers, false names, synthetic or otherwise, that he described. And from a prosecutor's standpoint, it's difficult for law enforcement, not only the prosecutors but the agencies that are investigating these crimes, to be able to bring these cases together until they are made aware of a problem that is focused in maybe a specific area.

And I'm thinking specifically of an instance of a prosecution of a credit card bust-out scheme that I did in Los Angeles where it targeted a specific area of Southern California. Had these individuals spent only a short time in that particular area and moved on to another one, it would have been practically impossible to discover them. But, instead, they used two physicians and the patient list of physicians, as Chris pointed out, to use variations of their Social Security numbers and their names or to make up names and, in some cases, make up Social Security numbers.

But they went a step further and added these point of sale machines, or POS machines, and what I'm talking about, for those of you that may not know, are the machines that swipe your credit cards. So, when you go to a store or you got to a restaurant and they give your card and they swipe the card, that's a point of sale machine. These individuals were smart enough to take over a small deli and run it into the ground, and when they left that deli, they took the point of sale machine and they were able to create a couple of shell companies and secure two other point of sale machines.

And when we finally -- when law enforcement finally caught on to this and when there was a search warrant issued and their residence searched, in each bedroom there's a point of sale machine. And that's taking a credit card and just swiping it and creating money. And what they would do is take a few of the credit cards and use those as the base cards and the base accounts, and they would gradually build those cards up. That's why sometimes you will see an account that was opened two or three years earlier, they're very patient, and they'll continue to use those accounts until they increase the credit limits on those accounts. And then they'll bust those accounts out.

And when we took down these individuals and

arrested them and searched their residence, we found 800 credit cards. And out of the 800, there were almost 400 that had not yet been activated, but the others were in some form of activation.

In terms of prosecuting a case like that, it's very easy once you identify and can focus in on the problem. But it's getting to the point where you identify that the problem exists because there are so many accounts and so many credit cards out there, that unless you see a pattern or unless they create some sort of mistake it's difficult to have law enforcement present a prosecutor with a case.

One thing I'd like to also address in terms of like nickel-and-dime prosecutions, that's a good point. In most districts around the country for U.S. attorneys, there are limits on the amount of monetary loss for acceptance of a case. They're called guidelines for each office. In smaller districts those guidelines are smaller. In larger districts, such as the Central District of California, they are much larger.

For example, in the Southern District of West Virginia, an identity theft case guideline would be $30,000 in loss. In Los Angeles, it's $750,000. Now, that sounds a little worse than it actually is because on identity theft cases, it's not always driven by guideline

laws. It can be a unique circumstance. Those are only guidelines. And the prosecutors that are in each of those offices now have an identity theft coordinator that they can take these cases to because that's part of the President's Initiative on Identity Theft that -- Joan, I think you had worked on over at main Justice.

MS. MEYER: So, in other words, you're talking about looking at maybe the type of victim, if it's specifically a vulnerable victim like someone -- an elderly victim --

MR. WEBB: That's correct.

MS. MEYER: You might take that, even if it's under the guidelines?

MR. WEBB: Absolutely. So that more identity theft cases are prosecuted.

One last point I'd like to make. In terms of percentages of reported identity theft crimes and how you determine whether someone knows the individual or doesn't know the individual, for law enforcement, they report those crimes because it's been investigated. And that's how they know who committed that crime. There are many identity theft crimes out there that go unprosecuted because no one knows who committed those crimes.

So, it's much easier to gauge who it was and the relationship between the people whose identities are

stolen and those who are the thieves once you know who it is to prosecute.

MS. MEYER: And just --

MR. SULLIVAN: Could I chime in here?

MS. MEYER: Sure, Bob.

MR. SULLIVAN: Thanks. I just wanted to say a quick thing to support what Chris suggested in his paper about reporting for identity fraud in particular. I don't think that there's really much argument that the notification law from California, which spread across the country, was the single seminal event in this whole public debate we have on privacy and on data theft and on data retention. And without those rules, there's so much theft we wouldn't know about. And, in fact, I do know that European nations who have privacy laws that we admire, you know, frankly look at us as the model for that, because as this most recent U.K. incident portrayed, those companies have no requirement to tell people what happened.

So, I'm a really big fan of Chris' reporting suggestion, and here's why. There are people in the room sitting there right now who are currently sharing their Social Security number with someone else, and I can promise you that there are also people in the room who have more than one Social Security number attached to

them and they don't know. And that's a tremendous cause of distress. And it's one of the reasons that the problem is perpetuated.

And, finally, again, about notification, everyone should know about the T.J. Maxx incident, and one of the things that I often will talk about is the fact the data is collected and kept infinitely by many companies. One of the problems at T.J. Maxx was that they had just not credit card numbers but even driver's license numbers for product returns and some of them were five years old, and people had no idea that T.J. Maxx still had their driver's license number.

So, a shining light on this problem will really get us much closer, I think, to the solution that we all want. So, I hope people take a look at Chris' paper.

MS. MEYER: Bob, I know that you've said that you've looked at a lot of studies. How solid do you think the data is about how often identity theft actually happens?

MR. SULLIVAN: You know, it's really tricky because we still -- every meeting I go to like this we spend a couple hours trying to figure out what identity theft is. We're still struggling with the definition. So, you know, whether it's nine million or ten million or whether it's going up or down or sideways, one thing is

clear, I mean, millions of people are still victims every year. And because I can't see all of you, I don't know how many people are in the room, but whenever I'm in a room of 25 people, I always ask the question and there's always at least one or two people who raise their hand. So, in the tens of millions is probably a pretty solid number.

MS. MEYER: Now, we didn't talk about what kinds of crimes are committed if a thief obtains an SSN. John, could you talk a little bit about that?

MR. WEBB: The most common types of crimes that we see are crimes where individuals have had their accounts hijacked. Someone has used a Social Security number to take over -- whether it's a credit card number or bank account, to hijack an open account or to open a new account. A Social Security number can be used for any purpose, and it's so widely used now, you can't have anything such as a utility service or you can't be employed, you can't file your tax return, you can't get a cell phone, you can't do anything without a Social Security number.

So, practically anything that you can use to get a Social Security number could be a potential identity theft crime. Most of the time we see it where people are taking over credit cards or taking over bank

accounts and using it that way.

MS. MEYER: In your experience -- and this is directed to any of the panelists -- how long does it take for a victim of ID theft to clean up credit? Tell us a horror story.

MR. WEBB: Can I respond?

MS. MEYER: Yes.

MR. WEBB: I'll tell you a personal horror story. It never ends, I don't think. My identity was stolen in 1990, or '91. I still deal with that to this day whether it's through my security clearances with the Department of Justice or through credit in some way. It's a horrible problem to have to deal with. And the cost in time and hours alone, not to mention the money that you waste trying to get these things corrected, is just horrific. I don't know that it ever goes away, but I do know that there are ways now through, thankfully, the FTC that will help you clear it up much faster than you would otherwise be faced with.

MS. BELLAMY: I do think it can take a long time. I mean, I've had certainly credit cards stolen and an account takeover. I don't know if I would necessarily call those identity theft. In my cases, it was very easy to fix. I mailed an American Express payment one time by check and the mailroom stole it, and then I got a nasty

note from American Express saying you didn't pay your bill. And I was like, yes, I did, and then there were like 800 pagers on it and the criminal wasn't so smart this time. He actually bought some plane tickets and, so, his name was right there. So, we were actually able to get that guy.

I do think it can take a long time and I think the thing that's really helped people is really to sign up for credit monitoring, and I think that the credit bureaus are coming down on prices. I think companies are starting to offer that as a benefit, and I think that that really helps because then you can find out about if there's another credit card potentially attached. Sometimes it's a mistake. I mean, someone will fat finger a number and you'll get connected to somebody else's card. Frequently, if you live in a household with a junior or senior the credit apps or the credit reports are somehow connected. So, I think that that's really a terrific way.

Plus there's the free -- you can apply for a free credit report and get that and just look at it. I don't think consumers understand that a lot because I talk to people all the time when they've had issues and they're unaware that there are even credit bureaus, I mean, which then horrifies them if they don't understand

how that financial process works. And I think you kind of miss that when you practice in this area and you talk to people all day who know these things. I think you sometimes overestimate the knowledge that people have about how it works and why all this information is used. So, I think that's terrific.

And for a future topic, I am reasonably concerned about -- I don't think holds -- from talking to people I don't think holds particularly work and I don't think freezes are a solution at all, and I'm concerned about the number of people who think that freezes are the easy way out.

MS. MEYER: Does anybody out there have a question for the panelists? Sir?

MR. MEZISTRANO: I'm with the American Payroll Association. I have a question for Chris. The American Payroll Association, our members, of course, are using Social Security numbers all the time and, you know, paying employees and issuing W-2s, and one of the things that our members do is we will verify employees' names and numbers against the Social Security Administration's database.

Chris, you mentioned there are some private databases out there for verification. Can you describe those? And then I have a follow-up question on that.

MR. HOOFNAGLE: Almost all the consumer reporting agencies offer add-on verification tools. For the credit granting context, they usually cost more, but retailers are free to sign up to use these tools which are effective in stemming some theft. And I think they would certainly get the problem where a Social Security number is used with a fake name.

MR. MEZISTRANO: So, you're saying that would be a solution to the synthetic identity theft or it would at least take a big bite out of it?

MR. HOOFNAGLE: I think some of it. And I think that ID analytics could speak to that issue more precisely than I can and they're speaking later today.

MS. MEYER: Ma'am?

MS. CRANE: Hi, my name is Joanna Crane. I work at the Federal Trade Commission. And I have one observation and one question. Chris, when you were talking about synthetic ID theft, if the idea is that those synthetic IDs don't affect an individual victim or aren't picked up by the surveys that we do, then the problem would be really vast because when we do our surveys we pick up -- if it was, in fact, just 12 percent of the identity theft incidents, we did pick up 8.3 million people who have had at least one account affected which suggests there would be another 704 million

accounts out there that we didn't pick up. That boggles my mind.

Similarly, with the dollars, if we only picked up about 25 percent of it, then there would be another 75 billion in losses that we didn't pick up. And that would just be for 2005. So, I think there's some way that ID Analytics needs to take account for the fact that although there was a mismatch between the name and the Social Security number, someone found out about it and was able to respond to surveys such as ours when we asked victims and were able to say, yes, I'm a victim of identity theft and these accounts were opened and this money was lost, because otherwise, I just think the economy would be in far worse shape than it is, I mean, somehow.

And I have a question for John Webb. John, you mentioned a couple of things that could really impact Social Security number compromise, like skimming or people stealing pre-approved credit offers and obtaining credit, I guess, or someone's driver's license or credit card or checks being lost, and those would translate into obtaining their Social Security number. And I was just wondering how that would happen.

MR. WEBB: There are Internet chatrooms where individuals can match up information. They can match up

Social Security numbers with names, with DOBs. They even have access, in some instances, to public records. And as everyone here, I'm sure, knows, public records are available to almost anyone. And there has been some movement to try and restrict numbers such as Social Security numbers off of the public records in courthouses, but that really hasn't happened in very many places.

As a matter of fact, the only instance that I know of it is where we are required, through the federal system, to redact an individual's Social Security number on any documents that we file with the courts. But if you wanted to go and see the mortgage lists or the marriage licenses or any number of other private personal documents, you can still do that in most courthouses.

MS. CRANE: But how would -- I mean, you could do that without getting their credit card or a stolen check. They could just have your name.

I was just wondering how -- you could do that with public records only knowing their name or their name and address. So, I was just wondering how the skimming or the pre-approved credit card or stealing so much credit card would facilitate anything beyond accessing public records which people can sort of do on their own?

MR. WEBB: For example, skimming, what we found

in many of the skimming cases, the skimming is done at a restaurant or retail business or some other place where they have point of sale machines. But it's very unusual for that skimming to actually be processed right there. It's usually downloaded and then uploaded to the Internet and it goes again out over the Internet to the various locations where people use this information and they match it up, and that's how we've been seeing it used through skimming.

And the same thing through credit applications, those applications are pre-approved, they sign those and just send them back into the companies.

MR. BLAKLEY: Hi, Chris, Bob Blakley from the Burton Group. It seems to me that with respect to synthetic identity theft I can distinguish at least three cases that might be different in difficulty of detection and impact on victims.

The first would be a combination of a living person's valid Social Security number with other synthetic details like a false name and address. The second would be the combination of the valid Social Security number of a deceased person with a synthetic name and address. And the third would be construction of a new sort of syntactically valid but not yet issued Social Security number with false name and address.

Do you have any information about the prevalence of these three modes of synthesis of identities and, if so, you know, sort of difficulty of detection and impact?

MR. HOOFNAGLE: No, the clear answer is just no, I don't. But that is a great point. I think several of the flavors you mentioned in that taxonomy have been done and they've been demonstrated that it's possible to engage in those various flavors of fraud, but the extent to which it's happened is unknown. And, you know, to follow up on Joanna Crane's point earlier, this is why I think it's really important that we come up with consistent definitions for this field so that we can kind of map out the problem.

In having this conversation, we still use different words to describe the same things. And part of it is politically motivated, I mean, you'll see that the banks are trying to narrow the definition so it's only new account fraud and not account takeover. And, so, that really confuses the situation. It would help to come up with a common set of definitions.

MS. McCULLOUGH: Hi, my name is Catherine McCullough. And a couple of years ago -- actually several of you here, I can see, probably know me from the Hill. I was with the Senate Commerce Committee and

several of you lobbied me when we were writing the Identity Theft Bill. So, I would like to say hi to you. I'm now in the private sector, so now you can take your hits very freely.

But I have a question for Ms. Bellamy. We really worked hard to try to come up with some kind of compromise language on how you define real harm when it came to notification. And, you know, we didn't want to penalize businesses, we didn't want them to be secondary victims. But, on the other hand, we felt we had to come up with some sort of notification. So, where do you think the real harm standard should be?

MS. BELLAMY: Real harm as to when to notify?

MS. McCULLOUGH: Yes.

MS. BELLAMY: I think it's very difficult to figure out what that is. And I think that the risks or the factors that you would look at would have to be, is there actual theft, has something actually happened.

I heard a statistic which I couldn't believe, which was if you're involved in one of these really large, like laptop thefts, or something like this one in England that happened that you're more likely to be hit on the head by a meteor than you are to experience identity theft from having a laptop stolen. It just seemed like that couldn't be true, that just seemed crazy

to me.

But I think that's a distinction that we're trying to draw is there ought to be a difference between something like that happening and somebody who is actually somewhere stealing it or there's more evidence of people stealing it, and I don't know what that is. I do get frustrated because we get a lot of calls both from the FTC and other places saying, well, we get a lot of calls about Home Depot. I'm like, well, it's not really Home Depot, it's Home Depot, Wal-Mart and all these other cards and a lot of people will buy the gift cards and then ask them do these phishing kind of things online and say, if you fill this big long thing, include your Social Security number and all this, you know, bank account information and everything, then we'll give you a Home Depot gift certificate. Well, that's not us, but we get a lot of people who think it is, unfortunately.

And there’s a new scam out there right now where you’re supposed to be in some type of focus group and fill out this thing and then it's in combination with one of those scams where they'll send you a check for $4,000 and then you have to send them $500. We don't do those kinds of things, either, but those particular things involved both Wal-Mart and Home Depot, supposedly were behind that.

So, you know, it is really a problem and it's hard to come up with what works and is fair to everybody.

MR. HOOFNAGLE: If I could quickly address this great question. One first question is why should the standard be harm-based? You might think about consumer detriment instead which is a standard under the deception language of the FTC Act. That's one thought.

Another is that harms are really broader than identity theft. So, you might have read that 10 private investigators were just indicted in Washington by the Assistant Attorney General there. And what they were doing is they were using Social Security numbers because they're basically the password that controls everything. As Mr. Webb noted, they're really the keys to the kingdom in order to get information such as people's tax records and their medical records. They're charged $500 for a full financial research job. Less for other types of information.

In those cases, it's not -- it's probably not identity theft that's afoot, it's probably lawyers who are hiring these private investigators to go after potential defendants and witnesses.

So, I think the idea of harm has to be broader than identity theft. It's also this kind of random invasion of privacy. But it's also issues such as

stalking and domestic violence. Breaches occur for all of these reasons and it's hard to measure their occurrence. I will say that the Assistant Attorney General -- it's the AUSA, excuse me, from Washington did say that the information of 12,000 people were stolen by this ring of identity thieves -- excuse me, private investigators.

The other point I'd make is size doesn't matter. A small breach can be just as risky as a large breach because identity theft is a manual process. And as Mr. Webb pointed out, they had a lot of credit cards in this one scheme, but a lot of them hadn't even been processed yet. It takes time.

And then, finally, defaults matter. If the default is to prove a negative or if the default is to prove that there is harm, I think we're going to see there's a lot of investment in forensic experts who come in and say there was no problem here. And we all know how the expert game works.

MS. MEYER: Well, Chris, do you have any sense of where your notification threshold would be to the consumer?

MR. HOOFNAGLE: Well, I do think that it makes sense to have a risk-based standard, but I think what's more important is to have public reporting of all

breaches. Just have a central database maybe administered by our friends at the FTC who need more money. Because security experts literally learn from each other's mistakes and we would have an aggregate of benefit by knowing basic information about security breaches.

MS. McCULLOUGH: Thank you for your excellent reply. And I have to say that having been on a team that oversaw several agencies on the Commerce Committee, hands down the FTC was our favorite. They do a terrific, professional job, and I agree, get them more money, they deserve it.

MS. BOCRA: Hi, my name is Nicole Bocra and I want to thank the panel and the FTC for putting on this workshop.

I believe the majority of the panel had mentioned that typically law enforcement and the private companies have thresholds in which they won't investigate something further, if it falls below a particular threshold or if someone isn't part of a particular class that may be a victim as in an elderly individual.

So, do you have recommendations for the consumer that is a victim of identity theft to what they can do to help themselves out?

MS. BELLAMY: We work very closely with anybody

who calls. There doesn't have to be a limit or anything. We work very closely with them and we've developed good relationships with the credit bureaus.

Sometimes it is harder to call in, as a consumer, when you're calling in by yourself just because a lot of people don't understand the inquiries. And, so, if they see an inquiry on there, they're convinced that their identity's been stolen. And sometimes that's the case. Most times, it isn't. And, so, we work closely with them, we get on the phone with them, get on the phone with the credit bureau and try to work those kinds of things out with them.

We also involve our IT security and corporate security and a number of them have law enforcement backgrounds with the Secret Service or the FBI, and, so, they still have contacts. We work closely with law enforcement to try to turn over all those stones to make sure that the issues are addressed.

And if somebody wants to e-mail me if they have a particular issue, that's fine, too. I mean, we have privacy@homedepot.com e-mail if somebody feels that something's happened. Sometimes it's very difficult, though, because you get somebody who calls and says, well, I'm doing kitchen remodels, so I've been there a whole lot, and I think my identity was stolen there.

Just because you frequent a place a lot doesn't necessarily mean your identity was stolen there.

I personally was actually horrified last night when I checked into the hotel because they actually ran a physical copy of my credit card with one of those -- whatever you call those things, I didn't even know that they had them any more, and I would much rather have my number held by a point of sale machine or that type of thing than I would have it floating around in paper or to give it to somebody over the phone.

MS. MEYER: All right, we'll take one more question. Sir?

MR. CLAWSON: My name is Pat Clawson, I'm a investigative reporter and I'm also a credentialed private investigator. I live between Washington, D.C. and Michigan.

Mr. Hoofnagle mentioned the alleged private investigators in Seattle who were indicted a few days ago. It's my understanding virtually none of those people were actually licensed private investigators, they were basically information brokers, but somehow they've gotten the private investigator tag slapped on them by the press.

Credentialed private investigators do things honestly and ethically. All right? The stuff that went

on that was alleged in the Seattle indictment is nothing that any of us would take part in.

The problem with identity theft basically boils down to financial losses on credit cards and bank accounts. That accounts probably for over 90, 95 percent of all cases of identity theft. The financial institutions are not doing enough to police their own act.

I would like to see the FTC and the federal government adopt a private right of action for private citizens who are victims of identity theft to be able to go after the perpetrators with a very serious level of mandatory minimum fine that you're going to be awarded in the form of damages. We already have that in copyright law. If there's an infringement in copyright law, we're looking at a minimum of $25,000 per infringement. The Fair Credit Reporting Act, the Fair Debt Collections Practices Act, all of those have a mandatory minimum -- in those cases, very minimum -- level of damages due.

Law enforcement can't handle this problem. There's too much of it. Private investigators help people deal with identity theft far more than law enforcement does. But many of the proposals that are pending here in Washington would cut off our ability to work with these people, to work with citizens who have

been victimized. We need to have some kind of a statute that gives private citizens a right of action, an expanded discovery power and a minimum mandatory fine.

In my own case, about a year ago, I got called one Saturday afternoon by Best Buy wanting to know about big screen TVs that were being charged onto my credit card account. Well, I hadn't bought any. They were calling from Minnesota. I was in Michigan at the time, all right? And after some discussion with their security staff, I learned that the TVs were being shipped to an address in New York. I wanted the information so I could file a private civil suit against the perpetrators who were misusing my credit card information. Best Buy refused to give me any information at all to allow me to be able to pursue any type of a private civil action.

We prosecute antitrust, we prosecute racketeering, we prosecute most fraud in this country by civil means. We need to have that ability as well in this area.

MS. MEYER: Does anyone have any comment on that?

MS. OWENS: I understand that you said that identity theft, the financial was about 95 percent of the losses. Is that what you were saying?

(Participant not at microphone)

MR. CLAWSON: The studies done by the U.S. Government (inaudible) with other agencies shows roughly 90 percent of all so-called identify fraud or identify theft principally involves losses involving credit cards and bank accounts, and generally, those losses are (inaudible) $5,000.

MS. OWENS: Yeah. But there's another --

MR. CLAWSON: (Inaudible).

MS. OWENS: Is there any percentage that you can actually -- I guess you can speak to this, Chris, in reference to the fact that you have your medical losses and you have your character assassinations, and then you also have your driver's license, those percentages are not even being mentioned in reference to how that actually causes a real --

MS. MEYER: Chris, is there any data regarding this?

MR. HOOFNAGLE: Yeah, the FTC report speaks to this.

MS. MEYER: Okay.

MS. OWENS: Because, actually, the actual -- which the FTC put out is about 26 percent is actually your financial. So, I just wanted to speak to that in reference to that we need and we must continue not to levy this on the individual because most people don't

have the credentials that this gentleman has in order to correct what's going on, they have other lives, they have other things that go on. So, it has to, you know, come down to what we're doing today in order to get a better understanding of how we can actually help the consumer and not hinder the consumer putting something of that magnitude on them to try to correct their own identity losses. It's just too huge.

MS. MEYER: Well, I encourage everyone to go to the FTC website and do some reading, and I thank the panelists today for their advice and I think we should all give them a hand.

(Applause.)

PANEL 2: SSN DISPLAY AND USE AS AN INTERNAL IDENTIFIER

MS. SINGH: Good morning, I'm Pavneet Singh with the Federal Trade Commission. In the last panel, we had a great discussion about the risks of using Social Security numbers. Over the next few panels, we're going to talk about some of the ways and reasons why organizations find it beneficial to use SSNs and also some alternatives to those uses of SSNs.

In this panel, in particular, we're hoping to focus specifically on the display of SSNs, how SSNs are used by organizations internally to identify individuals to match their information to them and some of the efforts that are being made to move away from these uses of SSNs.

We have a very distinguished group with us this morning. First, we'll have speaking Steve Sakamoto-Wengel, Assistant Attorney General and Deputy Chief of the Consumer Protection Division of the Maryland AG's Office.

Next, we'll have Kim Gray, Chief Privacy Officer of Highmark. Then Jim Davis, Associate Vice Chancellor for Information Technology and CIO of UCLA. Next, we'll have Kim Duncan, Vice President of Enterprise Fraud Management at SunTrust Bank. And, finally, Bill Schaumann, Senior Manager at Ernst & Young.

We're going to start with a brief presentation from each panelist and then we'll open it up for questions. And I ask that the panelists all speak into the mics when they make their presentations

And, first, we'll hear from Steve.

MR. SAKAMOTO-WENGEL: Thank you very much. I'm basically here to talk about Maryland's Social Security Number Protection Act which is similar to laws in a number of other states. Maryland's Social Security Number Protection Act was first enacted by Maryland's General Assembly in 2004 and was more or less based on California, which had passed one of the first Social Security Number Protection Acts.

It prohibits a person, other than a state or local government, from publicly posting or displaying an individual's Social Security number. The law prohibits printing Social Security numbers on a card that's required to access products or services; it prohibits requiring an individual to transmit his or her Social Security number over the Internet without a secure connection and encryption; prohibits requiring an individual to use a Social Security number to access a website unless some other unique personal identifier or authentication device is also used.

Now, the bill contains exemptions for any

requirement to use or release a Social Security number pursuant to state or federal law; the inclusion of a Social Security number in an application, form or document sent by mail that is part of an application or enrollment process or to establish, amend, terminate an account, contract or policy or to confirm the accuracy of an individual's Social Security number or for internal verification and administration purposes.

Now, it also provided that use of a Social Security number prior to enactment of the statute can be continued if the use was continuous and the person who is using it provides the individual with an annual disclosure form advising them of the right to discontinue that use. And the law further provided that a person may not be denied products or services because of a request to discontinue use of their Social Security number.

Although there was little opposition during the legislative session, the governor vetoed the bill at the request of insurance companies who were concerned that they communicate often with their clients via the Internet or via facsimile and they needed to use Social Security numbers as an identifier. Particularly, one insurance company mentioned service members overseas and that they would not be able to continue to do that under the law. So that bill was vetoed.

During the 2005 legislative session, the bill was amended to allow the use of a Social Security number by e-mail or facsimile transmission as part of the application process. So, the one that originally was limited to mail was expanded to allow facsimile or e-mail transmission. The bill also provided that an Internet service provider or a telecommunications company would not be held liable for the transmission of a Social Security number just using their Internet service connection or using their phone lines, as long as they're not the ones transmitting it. The bill was passed and signed and became effective January 1st, 2006.

At least 17 other states also restrict the printing of Social Security numbers on ID cards that are required to access products or services. Twenty other states prohibit intentionally communicating Social Security numbers to the public or the intentional public posting and display of Social Security numbers. Fifteen states restrict the mailing of Social Security numbers.

Maryland's Consumer Protection Division has not heard that this law has been unduly burdensome on Maryland businesses. We've been in contact with Maryland's Retailers Association, with the Chamber of Commerce, and they really have not found it's been difficult to comply with the law, I guess partly because

of the exemptions that kind of swallow the whole in some cases.

Also, we have not had issues with health insurance companies who have needed to transfer, no longer using Social Security numbers as medical record numbers. They've managed to implement that without much difficulty.

Who we do continue to hear from are consumers who are more aware of keeping their Social Security numbers private and having businesses continue to request Social Security numbers to complete transactions. And we continue to receive, you know, a number of complaints each year from consumers who are concerned about that. In most of the cases the request is still, you know, authorized under the law. So, there's no violation there, but we do have consumers who are concerned as they become more aware of it.

I guess the one thing that we experienced is in our own effort. In Maryland's Consumer Protection Division, we have a registration program for homebuilders. Maryland homebuilders are required to be registered with the Consumer Protection Division. As part of the registration process, we're required to collect Social Security numbers from those homebuilders. Not really wanting to have to collect this information

any more and not wanting to have to maintain it in our databases, we sought to amend the law so that we would no longer have to collect it only to find out that because of federal law, if we stopped collecting that information, Maryland would have lost about half a million dollars in federal funding because they're required to collect it as part of any kind of license application. And, so, our own efforts to restrict our own use of Social Security numbers was limited by federal law.

So, we realize that businesses have come to rely upon Social Security numbers identification in order to provide credit. But we really have been trying to work with businesses to determine when they really need it and when they don't. I mean, if somebody is opening a credit account, yes, you're going to need the Social Security number to check the credit. But there are other instances where people are continuing to collect it out of habit and we're trying to discourage that among Maryland businesses.

So, that was the Maryland Social Security Number Protection Act. Like I said, a lot of states have similar provisions. Thank you.

MS. SINGH: Thank you. Kim?

MS. GRAY: Okay, can everyone hear me? I tend

not to be real quiet, so I don't think that's ever a problem.

Just a little bit of background information because you may not be familiar with the company named Highmark. The company that I work for is a member of the Blue Cross/Blue Shield Association. And while we are based in Pennsylvania, we actually have national account business that places us in all 50 states. Hence, when California and other states started looking at Social Security legislation, we paid attention because, of course, most of those states, it's based upon the residency of that particular individual.

So, what I'd like to talk about briefly this morning are two topics. The first is what we have done, Highmark has done, and how we did get away from the use of SSNs several years ago. And then I'd like to talk about why we still need SSNs, however, for internal uses as a health insurance company and maybe generate some discussion on those needs for internal usage.

As I mentioned, we are in all 50 states and we do pay very close attention to what's going on across the country, and several years ago, right around the same time that good old HIPAA Privacy Rule implementation was taking place and we were spending millions of dollars on the HIPAA privacy implementation, we were watching very

carefully what was going on in California, and at the same time, our group accounts, those who get insurance for their employees, were contacting us. Everyone was quite concerned about the use of Social Security numbers and just how safe that was.

And the group accounts were coming to us saying, Highmark, what are you going to do about this? I'm watching legislation and talking to our CIO kind of at the same time saying, you know that group number identifier issue you're going to get away from, let me tell you what I think. I'm seeing California, I'm seeing I think at the time Arizona and Utah were on the radar screens as well. I think we need to get away from SSNs on ID cards. And, fortunately, my CIO also agreed with me that that was a good thing to do despite what we perceived as a large output of money to take care of that.

Thankfully, we did get started on the project in 2001, concurrently with all the HIPAA things going on at the same time. And I say "fortunately," because before too long, the other states did start passing that and it did, of course, become a mandate which did, of course, make it a lot easier for us to get the funding.

Those of you in corporations where perhaps dollars aren't so readily coming to you for things like

this, it's always helpful when you have a mandate. You hate them on the one hand, and on the other hand, they're a great thing because you have to find the money somehow.

So, speaking of money, it did take us $9.8 million to get away from the use of SSNs as an identifier on an insurance card and we went to what we call a U-M-I or UMI, Unique Member Identifier, which is, I believe, a 16-digit number that we generate. It is not related to SSNs. The reason for the 16 digits was at about the same time we were doing this, the Blue Cross/Blue Shield Association was paying some attention, too. Mainly because we were telling them you should pay some attention to this. Therefore, we had to come up with a numbering system that matched all the Blue Cross/Blue Shield plans, because even though we're independent, we are all interrelated as well.

So, we came up with the 16-digit number. Gosh knows we didn't want to have nine because nine looks like an SSN, and if it's not, it could be mistaken to be one, and a whole lot of other factors. So, it's alphanumeric, 16 digits.

It took us a good two years to roll that out and we rolled it out to our own employees first. Those of us working for Highmark were the first ones to get this. So, all the problems and the testing that happened

in real time happened with us. But I can say it did go pretty well.

The issues that we did have revolved primarily around our group account customers. The very people who came to us and said, please, fix something; we don't want to be always using SSNs for our employees were also the same ones who came to us and said, well, we don't want your number, we want to generate our own numbers, we want unique member identifiers. And, of course, that becomes problematic because you have account XYZ over here and ABC over here and they have different numbers and it makes for a lot of paperwork and it's very inefficient.

Another issue closely related to that is we are a pretty big Blue Cross/Blue Shield affiliate at the parent level. But we also have a lot of subsidiaries that are for-profit and do all kinds of other things. We have a dental insurance company, we have a vision insurance company, and these two are all national presences. We have a life and casualty company and we have all kind of things that really don't have a whole lot of things to do with insurance. Workers' comp kinds of relationship management with providers. You name it, we have all kinds of things.

At the time, because I was so busy and my Chief Privacy Officer -- we were all overseeing the HIPAA

implementation and kind of keeping my eye on this as well, when the subsidiaries came to me and said, gosh, Kim, do we have to do this the same way, the same thing and everything else and our CIO saying, gosh, Kim, I don't want to donate money to them as well, you know, if they're going to do this initiative, they need to ante up as well, we kind of allowed the subsidiaries to address the issue as they saw fit. Not such a smart move.

In hindsight, we looked back and found out that our dental insurance company decided to go with a truncated SSN, last four digits, and all it took one state law to come out and say, uh-uh-uh, you're not going to do that. So, they had to go back and fix things later.

Another subsidiary chose to agree with its accounts, when the account said, oh, let us pick our own, they didn't want to make too many waves with the accounts, and they said okay and, of course, that got them into some problems later when they were, as I was describing a while ago, having different kinds of numbering systems and trying to make things match up.

But, generally, we have now been doing this since the end of 2003. Things, I can say, have gone relatively well as far as that goes. We have not had major snafus with the 16 digits or with interplan

relationships or anything along those lines. It was not a cheap undertaking, but I'm glad we did it when we did.

Having said all that, I'm going to segue into part two, however, which is why we still need to use SSNs internally, and that's probably the bigger challenge for everyone in the room, I'm guessing, in some form or fashion. Because SSNs have been so widely used over the years as an identifier and authenticator, making sure you're talking to the person you think you're talking to, it's very common for people, consumers, at the very least, to expect to be giving SSNs out to authenticate themselves sometimes. And, occasionally, when our customer service representatives are talking with a customer, that customer wants to give an SSN, they have that memorized, they don't have that UMI memorized, they have to go look for it, where's my card, oh, my daughter has it or whatever. So, there are many reasons why we need it internally.

In addition, when we're verifying our eligibility for government programs -- we are a Medicare carrier and intermediary. Medicare, of course, for coordination of benefits to see who is Medicare -- if Medicare is secondary payer and that kind of thing requires -- of course, Medicare beneficiary numbers have that Social Security number as part of what we call the

HIC number on their health insurance cards for Medicare. So, it's difficult to get away with that when you're trying to coordinate when Medicare pays and when private insurance pays.

HIPAA transactions and certain state laws still require that you actually use an SSN as part of that interchange of information when you're processing a claim, and private plan's the same thing. For coordinating benefits, maybe you've got accidents, you've had an accident and you've got some other kind of either homeowners or auto insurance picking up part of it, very often these other insurance companies are still using SSNs. That's their main great way to identify an individual because, oftentimes, you've got same name, living at the same address and you can even have twin situations with the same birth date and similar names. So, for many purposes, the SSN is still a very valid and good authenticator.

We track our payments to our providers. Of course, you know, when a provider, whether that be a hospital or doctor or whatever, submits a claim to insurance, we're paying that person. Well, 1099s are generated for IRS purposes; again, the SSN is needed for that particular provider in many cases for tracking 1099 purposes.

Other kinds of insurance, if you're getting disability benefits, sometimes you're needing to coordinate with another insurance company along that way and, again, you're having to use the SSN. And like I said, back to the consumer, that's probably the biggest thing, many of our customers who are wanting to use SSNs internally. Thank you.

MS. SINGH: Jim?

MR. DAVIS: Thanks very much. It's quite a pleasure to be here this morning.

I believe I'm the first one speaking from a situation in which we have experienced a large database breach. Many of you may be aware that UCLA had a breach of significant size back in November 2006 in which we notified 800,000 people. And one of the things I'd like to speak to this morning is basically how that changes the equation or the balance in the equation of risk versus benefit. So, already on the base of quite a bit of activity in terms of removal of the use of Social Security numbers, the intensity with which we have been looking at it this past year, also takes us into some, you know, some pretty interesting studies.

But just to set a historical perspective on this, UCLA actually started putting together alternative matching criteria and approaches, cross-referencing

approaches 30 years ago. So, we had those kinds of systems in place at that time. We put a university ID, similar to an HIC number, which was separate from the Social Security number, back in 1994 and actually that was a process that had begun in roughly 1992. It seems like one to two years seems to be the magic number for moving these through. So, for us it was a two-year effort.

You heard mention already about the California notification law back in 2003. That was a significant incentive for us and many others across the state to take a look, a hard look, at our practices, and at that time we had gone through and removed the use of Social Security numbers wherever it was simple to do so. We had removed them from display, had tightened access to systems, put in processes for inventories and so forth. And then, of course, as I mentioned, the breach occurred in 2006 and that intensified a re-review of what we had been doing.

One of the things I'd like to do today is just kind of give you a very real feel for a couple of examples. But I'd like to set the stage very, very briefly for that. If you look at the university overall, and you can slice and dice it several different ways, but the way we look at it is there are five big populations

on campus.

The first is there's payroll employees. We've heard much about them, the drivers for Social Security numbers, or as everyone has been talking about, IRS, employment department, payroll, earnings types of things.

There's clinical patients, so very similar to what Kim mentioned. The only thing I would add to what Kim had said is at a research university like ours, we also have the aspect of patients that are compensated. So, we have to deal with Social Security numbers on that basis.

We have another couple groups which are more community-based in the development, donor area, and then we have a very large university extension or continuing education program. Both of these have been long users of Social Security numbers for authentication and identification. For development, it was used for identifying lost alumni.

These are two examples in which two major units, two major populations were able to move out of the use of Social Security numbers on a day-to-day basis. And our external affairs or the development department was actually able to do this with about a one-year effort moving those processes through. Our extension process is in the process -- has this in process and, again, it's on

target for about a year to two-year effort.

The efforts invariably are not huge expenses, huge programming efforts, this sort of thing, but they are significant changes in the business processes and working them through with the communities, that's what becomes of interest.

Just picking on the external affairs a bit. You know, the difficulty here was in terms of looking for lost alumni. This particular unit had to work these kinds of processes through with a number of vendors. So, Alumni Finder, LexisNexis, these kinds of vendors were used and there was multiples of these that had to be worked through. This is where it becomes more difficult.

What I'd like to do this morning is concentrate on a particularly interesting population for us that's a little different than, I think, than general corporate financial populations, and that's past and current students and student applicants. These present some particularly interesting elements for this and I think it's populations that all of you can relate to.

If I put these in perspective, our security incident in which we notified 800,000 people, if you look at that particular database, 60 percent were current and former students, 30 percent were applicants and parents

of applicants, and only 10 percent were current and former employees. So, you can get a sense of the size of the populations.

But let me give you a little perspective on the students and the student applicant situation. First of all, UCLA gets about 90,000 applications per year of all types when you look at undergrad, graduate, transfer students and so forth. And the drivers for Social Security numbers in these populations are, as one would expect and as is in the FTC report, tax, IRS reporting, financial aid requirements, the student clearinghouse. Ninety percent of our students have financial aid. We're among that 90 percent of all universities that are participating with a student clearinghouse, National Student Loan Association, and so forth. So, all of this is just as was reported.

But the thing that's interesting here is if you look at the applicant records and the reason that we keep these, undergraduate records are purged every two years. Graduate records are purged every three to five years. But even with those kinds of purging protocols, at any given time, we have something on the order of 250,000 to 300,000 student applicant records in our database at any given time. And the real point here is these are rolling over every year. So, we have a new set every single

year, constantly turning over.

So, let me take a couple of contrasting scenarios given this picture. The first is transcript ordering. All of you are familiar with that. We tend to get on the order of 50,000 transcript order requests each year. If you look at these, 40,000 of them were after the UID and about 7,000 of them were before if I just look at 2006.

So, one of the things that we've been able to do is on something like transcript ordering, these are current students or past students and, so, we have a full record on the campus. So, it actually makes it quite possible to move to other kinds of authentication, knowledge-based authentication because we have the full record and have been able to do so. So, we have been doing this -- actually, the past couple years have accelerated it since the security breach. But at this point we are no longer requesting Social Security numbers for this often-used day-to-day kind of operation. And, so, we have just about been able to work the use of Social Security numbers to eliminate their use.

But let me contrast this with the applicant situation. Just looking at undergraduate applications, we get about 60,000 received over about a five-month period. If you take a look at the profile of these, 10

percent have UIDs. In other words, they have a prior affiliation of the university. So, most are new people to the campus.

If you look at this where we used Social Security numbers as an authenticator and an identifier, we still have 1 to 2 percent manual intervention. So, the Social Security number, in itself, is not a clear distinguisher, although it greatly helps. Please keep in mind the time aspects of this, because if you think about admissions and financial aid processing, it's very time urgent. People are really looking for their admission information, and we tend to be processing about 3,500 of these per night, you know, during the admissions process.

The other thing to point out is that this is our process for the assignment of the UID. So, one has to think about how do you get from a new population to this assignment. So, this authentication credentialing aspect that the Social Security number provides is very, very important to us for even moving forward with the UID.

Also, with this 10 percent that have a prior affiliation, we have to go in before we assign a UID and check and see if the record -- if that particular applicant has a prior record. We have prior employees, we have undergraduates apply for graduate school, we have

students who apply multiple times at the university. These all produce records that need to be checked out.

So, one of the things that we do authenticate, not only to Social Security numbers but also to other criteria, but please keep in mind the other thing that's interesting about the applicant pool is that the date of birth for many applicants is pretty much within one year. So, that also makes the date of birth a very hard -- it's a useful criteria but it’s not distinguishing in itself.

So, imagine this one without the SSN. First of all, if you take a look at the matching algorithm, but with no intent of digging into details, right now we match against Social Security number, primary name, secondary name, date of birth, gender, last name, first name and middle initial, and all of these are all changeable with the exception of the Social Security number.

So, if you look at the conflict situations with that particular criteria, there actually are, just the combinatorics, about 100 conflict situations that are possible. This is what leads to these manual interventions.

Again, keep in mind that if you have to distinguish between Dan and Daniel, Kathy and Katharine, there are many of those out there coming in from this

applicant pool.

So, the thing about this is the ability to uniquely identify an individual without the Social Security number becomes much, much more difficult in that situation. But one of the things that we're raising here is because it's a time-urgent process, we already have 1 to 2 percent manual interventions which translates into about 600 to 1,200 manual interventions per year. If we were to increase this any significant amount, now we're really bogging down the process and it becomes a major, major issue to resolve.

But that still doesn't solve the problem for us with respect to the fact that how do we, in fact, assign the UID, and that's where we need the outside or the external authentication. And for a new population at the outset of the relationship with the university, that Social Security number becomes very, very important.

So, the main point I'm trying to raise with these two contrasting examples is we can go through an operation like ours, we can remove Social Security numbers with the incentives that are out there. The balance of risk and benefit drives us very strongly towards this. But there are situations where this external identifier is actually vital and our ability to remove it from a business process standpoint actually

becomes very difficult without external help or working with this in a much, much broader context than just the university operations itself.

So, let me just stop there. Thanks.

MS. DUNCAN: Good morning. As Pavneet said, I'm Kim Duncan with SunTrust Bank, but I also am representing the financial services industry in general. I serve as the Chairperson for the BITS Fraud Reduction Steering Committee, which is an organization under the Financial Services Roundtable representing the largest financial institutions across the country.

One of the things that I wanted to point out in this morning's session is that banks are very heavily regulated. The regulators are our friends, but how we conduct business and what we do within our business is very closely supervised by both the federal regulators as well as our state legislators depending on the jurisdiction. We have to adhere to very specific state and federal requirements, many of which pertain to how we identify our clients, what we do, how we store the information that we obtain and what we do with that information.

Identification of our clients is also regulated. For example, the U.S. Patriot Act requires us to set up very specific customer identification programs.

CIP is essential to the way that we do business in today's environment. But at the end of the day, banks do collect Social Security numbers and we store those Social Security numbers and we do that for a variety of reasons, and we try to do that in a very safe and very secure way.

We use that Social Security number for many different types of things. One is for legal requirements. It is very much a part of our business to respond to things like garnishments and levies, court orders, escheatments of dormant and unused funds. We have to have the appropriate mechanism in order to respond to those types of things.

We collect and utilize Social Security numbers for fraud prevention and for fraud recognition. Detecting fraud at the front end and proactively identifying identity theft situations is key to what we do, and we use that Social Security number as an identifier in doing that.

Identification and authentication of our clients. Again, we're very regulated in how we do that, and another one of our financial services friends will be talking at a later session about the authentication process, but key to how we conduct our business in the banking environment.

We use it for credit. Credit's a key piece of

the business in the financial services world, and the identification of the applicant is done primarily through the use of the Social Security number and pulling that credit history. It's essential that we are providing credit to those that are creditworthy; that we're providing credit to those who are the true applicant, again getting back to the authentication piece. And credit is a key indicator of the use of our Social Security numbers.

We also use SSN for tax reporting. Again, on the credit side, we have to report that credit interest. But we also have earned interest, whether it's through our deposit accounts, through our investment accounts, a variety of different means, but reporting of interest and tax reporting is an essential piece of what we do.

But how do we do that? And why do we care about the use of the Social and what we need to do? Banks are constantly enhancing the process that we use in looking at Socials, in storing that information, and in the way that we utilize the piece of numeric value that is associated with that Social Security number. We are very concerned about the strength of the storage capacity, again, very regulated, under GLB. You know, we were very much told how strong our information security processes needed to be, what mechanisms needed to be

used, how we should encrypt that information, and how we should store the information.

So, providing protection to our clients is essential in the way that we use that information and we work hard to educate our clients as well. We're constantly trying to look at ways to provide information to the client on their own mechanisms for protecting themselves. The use of the Social Security number, while key to our business, is not something that needs to be out in the area of the mail.

Mr. Webb talked earlier about the fact that mail theft is key in the way identity theft is perpetrated. Financial institutions have worked very hard at either redacting or truncating Social Security numbers in printed material. Ten years ago, you might have seen Social Security numbers printed on bank statements. We've worked very diligently to make sure that those types of things are not occurring any longer. Printed material such as statements and pre-approved mailings and whatever other types of information may be provided to the client are oftentimes redacted, or at least truncated, so that that Social is not out there when the mail is stolen.

We also look at how we provide information to the client and how we are able to service the client.

The question was asked earlier about how lost wallets or stolen wallets and purses can translate into identity theft situations. What you need to think about in the capacity of why banks use Social as an authenticator or as an identifier of clients is that when you lose that wallet or you lose that purse, your first indication or your first thought is to call your financial institution to protect your cards, to protect your accounts, and to make sure that that perp is not out there utilizing your financial information.

Well, guess what, it's 11:00 on Saturday night and your bank's closed, you can't walk into a brick-and-mortar location. So, you're going to call the call center. And what we've put in place are processes so that our call center folks can authenticate you. But one of the ways that we need to do that is to be able to provide an absolute definitive mechanism to know that we're talking to you. And at SunTrust, and at many other organizations, we've done that through the creation of a customer identification number, a unique identifier that says that this is Kim Duncan who is a client of this bank.

But just like with the healthcare industry or the education area, that other 15, 16, 20-digit number is not one that is easily memorized, and adoption of the

identifier has been very, very slow and very difficult. We have associated a unique identifier with our clients, but at 11:00 on Saturday night when your wallet's been stolen and you're very, very upset, you're very cautious about getting yourself protected. The last thing that you can do is remember that other 14-digit number that was assigned to you by this financial institution and, oh, by the way, you probably have cards in your wallet that are associated with four or five different institutions, each of which may have a separate identifier.

So, if we were relying on a separate identifier for each financial institution, we're actually putting our clients, I think, at a bigger risk and we're providing a very big disservice to them by not having a quick and easy mechanism to be able to identify them. It's very, very difficult to have a unique identifier for all financial transactions.

But the key is what we do with that information on the inside. Again, you know, making sure that we are taking the appropriate steps to truncate that information and utilize it only when necessary, making sure that when our customers are victimized that there is a quick and easy way to help them.

Financial institutions responded several years

ago by the creation of ITAC, the Identity Theft Assistance Center. This has been a mechanism and an organization that has allowed us to service thousands of identity theft victims that have been reported to our financial organizations. It offers us the ability to have a one-stop shop. To give them the support that they need to walk them through the process of rebuilding, of unraveling the problems that exist when an identity theft situation occurs. Helping them with the liaison, with the law enforcement agencies; helping them with the creation of a uniform affidavit; making it as easy as possible for them to walk through that creation of fixing their problems.

And, then, the last thing that I want to mention about the financial services industry is we're still an employer. We have many employees, and we have to use that Social Security number as an identifier. We have to pay payroll taxes. We have to identify those employees. We have created unique employee identification numbers and that's helped. But we still have reporting obligations and we need to be able to utilize that as any other employer does and just need to make sure that we safeguard that and take the appropriate steps with our employees.

MR. SCHAUMANN: I actually have some slides to

show you today. I'm Bill Schaumann from Ernst & Young, part of their Risk Advisory Group where we work with customers to reduce multiple risk areas, one of which is personal information use.

I'm going to speak today specifically about once your company/organization has taken the step to go ahead and reduce the risk of a Social Security number within your organization, how do you do that? What is remediation? And what we see is remediation is basically changing applications and business processes to reduce the risk of identity theft. So, basically, what we're going to do is take the Social Security number out of the system where it's not needed.

You've heard numerous examples today where companies need it for outside -- other organizations that they work with, but there's many, many opportunities to reduce the risk. So, you want to remove it from systems and processes where it's not needed, and then when you do know where you're keeping it and you have a good identity map, then you can put security on those and make sure that only those people who have a need-to-know access have access to the Social Security number.

It's a large problem. It's complex. It's not simple. For the last 20 years in this country, since the advent of computers, we identified people by their Social

Security number. In our country, we only have one. Other countries have many identifiers. Brazil has nine government identifiers. We have one. So, we use it for everything, which is not a good plan.

So, it's in all systems, and all systems talk to some other system. No computer system stands by itself. Every system either has an output or an input. That can be a file extract, it can be a report, it could be a direct sequel connection to other systems, but nobody stands alone. So, there's dependencies between these applications. And when you go to remediate, you have to take those dependencies into consideration.

Your solutions may not be ready. If you're ready to say, okay, we're going to get rid of SSN, we now need an identifier to replace it with, there's a whole elaborate architecture and system that you have to put together that takes into consideration all the things of your business. It must be coordinated with VPOs and other third parties.

We've heard today where the healthcare industry has a lot of partners. And that information goes from your first location to your second to your third and there needs to be a common thread through there. So, you really have to think carefully, where can I take it out and where can't I take it out?

And the state regulations are different in every state, so there's a lot to consider where you do business. So, there's a lot of things that actually go into this mix.

The strategy that we have seen effectively used with many of our customers is, first, to develop a central program office within the organization that has executive support. This has to be a top-down executive decision because constantly you're going to come into contact with managers and directors who say, why am I doing this, I don't have this in my budget, this is expensive and I don't have reason to do that. Without the executive support, you're going to give those guys a way out. So, you need to do that.

Policy within the company. You have to have good, strong policy and practice, again, so that the people that you're working with have something to refer to and say, okay, I'm going to remove it here and I'm going to implement some encryption techniques here according to the policy.

Education of employees. I think we have heard a couple of examples today where people say, well, I have to have it, my system runs on it. That's true, but depending on what your policy says, you may not have to have it. Your system runs on it, which means we have to

fix that. But when you say you have to have it, if you deal -- one of our customers said their rule was if you deal with a government agency and you're sending information to a government agency, then you can have SSN. Otherwise, you go to the employee identifier.

So, there is a lot of training on how to handle data and getting your employees basically in the right frame of mind. To me, it's a way of thinking. If an employee sees a report with a SSN on it, they should question that. Why is this on here? Does this really need to be on here?

Getting your business partners involved. Getting them up to speed on your identifier. Now, depending on the complexity, that may or may not work. You referred to a situation where in the healthcare industry there is a connection between the companies and everybody wants to have their own identifier, there needs to be some more common ones, I think, is what it really comes down to.

And, then, finally, limit access to who needs it and apply controls where it's needed.

What we have is an approach, I kind of dub the big four only on this example because there's four major systems. With this technique it allows you to -- one of our kind of tenets is always that it doesn't break

anything, also. We can't get in the way of business doing business. These guys still got to do their jobs and we want to make sure we don't break anything.

But most companies have major systems of where their information comes from. In this example, it's timekeeping, an hourly payroll, a salary payroll and a People Soft. All the other outsourced processes, corporate applications and forms, all tie to some of these systems, and you can get major advances by working with these first.

We broke down the areas, corporate applications, so they may go through many different areas that are basically supported. And the reason I differentiate that from -- in this block, the forms and processes, local applications, because what we've also seen is there might be an output from a major system like People Soft has a standard person report. Well, once it hits the plant floor, the local security guard takes a copy of that and makes his own Excel spreadsheet and the administration lead in the certain department takes his copy. So, it kind of propagates out onto the floor and you see many, many different uses of it.

One of the most unusual uses we've seen is -- actually, it's part of the union contract states for seniority, to differentiate who has more seniority.

Let's say Steven and I want the same job, we're going to vie for it, we were hired on the same day, so our seniority is actually the same. Union rule says we'll post up a list of the names and the Social Security numbers and you break the tie with the last four of the Social Security number. So, there's stuff that's embedded in our culture that goes way back that takes time to change. You can't change a union rule overnight; you have to wait for the contract to be up.

This is the major way we're going to do this. The primary uses, as many of you may know, there's two. Primary key. So, if a Social Security number is a primary key in a database that means that database uses that as the key field and references it. So, all tables and databases all key off that field, and it's everywhere.

My alignment's a little off on my slide, I apologize. But here you see two Frank Jameses in different departments, one in collections, one in security, with different Social Security numbers. So, therefore, that person may be identified uniquely by the Social Security number.

There is also many, many reports, fields, extracts, files that have SSN in there informationally, it's in there just because. In this second example, the

key field is the department. So, a department supervisor may get this report and show his people broken out by what department they work for and the SSN is in there just because. It's always been in there, it's a good information, good way to have it in there, I don't really need it. That's an easy one to fix, you can just cut that right off.

So, what you have is these four systems that basically talk to -- ooh, boy that's ugly.

These four systems talk to many downstream applications and, so, the idea is how do you get SSNs throughout all those without breaking anything. And there's a technique that we developed that you basically go to the first system and your source has an application that it's sending a daily extract to. This might be a nightly file feed that goes down. They're both operating on Social Security numbers.

So, the first thing you want to do is you add your employee identifier to the source. So, now it has both. It's not operating on both, but it has both. You then can add the employee identifier to the downstream application and, finally, you create a new extract and then you finally remove -- oops, before you remove, you have to go through screens and reports.

And this is where the real work is, going

through the code of these applications to look at report headers and processes within here. You really have to dig deep and it makes estimating very difficult because when you look on the surface how complicated these systems are, some of these legacy mainframe systems that have been around since the sixties are very, very deep.

We had an example, we counted one as an application that we were going to remediate. It turned out within it there were six major subsystems, and as the account grew, there were almost 100,000 databases that needed to be addressed in this one system that we counted as one. So, it's very difficult to get to that point.

So, then, you can finally remove the SSN and, therefore, we've fixed this application without breaking it. Now, what you can do with the same time is you've now put the EIN into your main-time keeping source system, and one by one, using that same technique, you flip the applications down, not breaking anything.

So, I apologize for the animation, it got a little messed up there. The challenges really are executive, top-down, buy in. All applications have dependency, so you have to work very closely with other application teams of when the switch is going to happen, how they're going to happen.

One of the most challenging things, and this

actually challenges your identity management system within your corporation, is a very good SSN-to-employee match.

There are many population types; I think you heard Jim talk about population types. Population types within organizations, and then this one had employees, contractors, suppliers, retirees, sole surviving dependents. So, there's many different population types and your identity systems may assign different source identities depending on what requirements they have. So, that good match is difficult to do.

Accurate cost, as I said, is very difficult, and the policy must be in place to support the remediation so the people know why they're doing it. And all the populations we talked about. That's all I got. Thank you.

MS. SINGH: Thank you all for the presentations. I wanted to ask a few questions and then we can open it up to the audience for additional questions.

But one thing that struck me as I was listening to the presentations was this idea of allowing the use of SSNs for customer convenience, that even if you've transitioned away from using the SSN as your primary identifier, you would still allow your customers or your

students to use the SSN in some situations. And I think Jim touched on this a little bit, but I'm wondering if others considered using additional identifiers or other identifiers instead of the SSN in those situations where a customer has forgotten. For instance, some combination of name, address, date of birth, and how well that would work in your situation. Maybe Kim Gray, do you want to start?

MS. GRAY: Yes, I'd be happy to address that. We do, in fact, allow for other identifiers as well. Typically, if we're going to get away from our unique member identifier, which is our first source of identification, and even with that we're asking for additional authenticators, we will, of course, ask for whatever it is that that particular individual might know off the top of his or her head. And it's very difficult sometimes, but you can get a date of birth and an address, perhaps. But, believe it or not, we even have issues of folks getting their addresses correct. You would be amazed at how many people don't know if they live on Waverly Drive or Waverly Street or Waverly Road and, I mean, you wouldn't think that's the case but that really is.

But very often when I spoke to convenience, that really is the member who’s calling us asking, can I

give you my SSN? It's so ingrained in the mindset that even if we were to ask the questions, the other authenticators, very often they still wish to be bringing that forth.

MR. SCHAUMANN: One of the other issues with those other authenticators is they change. So, my recent example is of the guy who says, what was your -- if it was a favorite question type thing, what's your favorite movie? Well, when he answered the question back in 1970, it was one thing and now it's something else. So, there are seven, I think, unique identifiers that don't ever change, things like your eye color, your city of birth, your birth order, I thought, is a very good one, and your height normally doesn't change except for maybe as we get older, it changes a little bit. But there are some things that don't require memory that can be used, and I think typically it's something you have and something you know.

So, any of these unique identifiers of what elementary school did you go to are also very good qualifiers.

MS. GRAY: If I could jump in and piggyback on that for just a second, however, because in our industry, why we would love to ask things like, you know, what is your favorite food or the things that are being discussed

right now, unfortunately most of what we know about our members comes from their employer. And we have run into situations where we are only given a certain amount of data from the employer that that individual may or may not want to share other kinds of information like what was your first school or whatever with their employer. So, we're somewhat limited to those things that we've gotten from the employer in most cases.

MR. SCHAUMANN: An additional challenge then becomes if you start as a U.S.-based company and then move global, you know, the rules change big-time as you go global. So, you have to really kind of consider all the pieces of global laws and regulations as you start to think about these things that you're collecting.

MS. DUNCAN: And I think, too, just the whole issue of issuing that additional identification number to the client is very time consuming, very costly, and the client adoption of that continues to be very slow. The memorization of another number, the expectation that we know who they are still remains there.

MS. SINGH: I mentioned that some of you must deal with foreign populations as customers or as your students and I'm wondering what that teaches you sort of about the difficulty of matching people when there is no SSN, at least for some of them, if they don't have an SSN

available either as a student or a customer.

Jim?

MR. DAVIS: I have to jump in on that one, I think. That one, of course, is very, very difficult. So, we really do depend on the SEVIS processes, which takes us into the visa and the passport. But it is basically all those other outside kinds of credentialing and identifiers that we would depend on, and that's a real mixed bag. So, it's just a very, very complex situation and one just has to go into a lot of detail to get to the bottom of that. But you depend heavily upon SEVA and those other credentialing processes.

MS. SINGH: Anyone else?

(No response.)

MS. SINGH: Steve, one thing I was hoping that you could discuss a little bit more are what types of consumer concerns you do hear, what are consumers most concerned about providing their SSNs and what situations do they register complaints about that?

MR. SAKAMOTO-WENGEL: Typically, the types of complaints that we do get are where a customer is trying to transact business with a retail store or over the Internet and they will, as part of the process, be asked for their -- they'll be asked for a whole lot of information. I mean, typically, now, businesses will be

asking for a phone number or a ZIP code or something else so that they can match you up to their own database, so they can be sending you marketing materials. But a lot of businesses also will ask for Social Security numbers sometimes because there's a credit transaction involved and sometimes just out of habit.

And consumers, like I said, are becoming more aware that this is something that can lead to identity theft and are being more protective with their personal information and are reluctant to give that in many cases. And, so, they'll be contacting our office and we'll contact the business and try to find out why they needed it and try to find out if it's a legitimate use or, again, it's something that's just out of habit. And if it's out of habit, we'll tell them, you know, you really should think of alternatives here, you don't really need to do this.

MS. SINGH: Anyone want to add anything?

MS. DUNCAN: Well, I think, from our perspective, most individuals expect a financial organization to ask for that type of information. So, we're somewhat fortunate in that standpoint.

But on the personal side, I'll share a story I shared with Pavneet earlier, and that is that -- I'm in war with our school board. And I think that there are

organizations, whether it is a retail organization or a camp or an education -- sorry, Jim -- entity that needs to think about not only do they need that information but how do they utilize it. I believe that in the education field, you do need it for a wide variety of reasons. But I got my son's high school report card in the mail, which is normal now because they don't trust the kids to bring them home. But in the mail it came to me in printed format with his full name, address, and nine-digit Social Security number on it.

So, I think you need to think about those types of things in the organizations that you're dealing with.

MR. SCHAUMANN: One thing I've seen that's actually the reverse of what you guys have said is within our organization that we're working for, once they heard about this and everybody started to see the light, everybody got on board. And that group of applications that I had, as we were going through one at a time, you know, we were only spending so much money a year to get this done.

So, people were saying, well, I'm not going to give you my Social Security number for anything any more. So, all the processes that weren't fixed yet they said, well, tough beans, go get my employee identifier and use that. So, the proper cadence has to go through as well.

MS. SINGH: Another thing I'm wondering, as all of you have gone through this process to transition, how important is it to look back at your historical customers and databases and change over those systems if you still have people in your systems or legacy databases that have SSNs that aren't active? What do you think about what factors to consider in deciding whether or not to transition these systems?

MR. SCHAUMANN: I can start off with that one. One of the things is, I think, is the cash, is money. So, if your choice is to fix an archived system or one that is active today obviously you're going to spend your money on the active one. So, we have actually said, you know, in certain cases for the archive, just make sure it's encrypted and then leave it alone and make sure your controls are good versus spending money on that.

MR. DAVIS: I just want to -- it pretty much echoes what Bill was saying. I mean, in our particular case we have, you know, legacy systems that have pretty embedded codes that go back in very deep ways when you have to unsort or unscramble these kinds of things and what we are finding is that, you know, generally speaking, we can do pretty good with internal processes if we have a record out there, and we can move towards some other rich record to take care of things.

But when we get into the middle of these kinds of codes, that actually is where the cost adds up and it becomes very difficult to deal with. But if I take something like transcript-ordering, which is the example I was talking about before, we do have the situation where -- we actually in 2006 had someone from 1940 asking for a transcript. In those kinds of cases, you know, they come very rare, so we can move pretty much off the use of the Social Security number as long as we just have it stored in a place that's very secure and use it in a very sparingly offline kind of fashion.

And that's the kind of movement that we've made in a number of these kinds of operations. You don't pull the eliminated, but you can consolidate and protect all of those.

MS. SINGH: One thing as we talk about consumer adoption and the difficulty of remembering these numbers, coming back to that point, we've heard this idea of perhaps having sector-specific ID numbers, perhaps having an ID number for the education sector, for the financial sector. I'm wondering what you think of that idea in terms of both what adoption would be like and would it be more beneficial to consumers and how difficult it would be practically to implement.

Kim Gray, do you want to start?

MS. GRAY: Sure, why not. That's a tough question. But I think one of the difficulties is going to wind up being there's so much crossover. As a health insurance company, for example, we're regulated by our state's department of health, by HHS at the federal level, and we're considered a financial institution for Gramm-Leach-Bliley purposes, and I think we can't be unique in that. I'm sure other industry segments have crossover as well and we all are kind of sitting here saying the same thing as it is right now even with the various industries.

Once again, too, I think if you look at it from the consumer's perspective, you're asking a consumer to now not just remember, you know, one set of numbers but 10 sets of numbers, I think you're going wind up with pushback from the consumer, but that's my two cents.

MR. SCHAUMANN: I refer back to the gentleman who spoke earlier about what identity theft is. You know, it comes down to credit and those accounts. And I could see other countries having separate numbers for separate -- the implementation would be vast and wide, I'm sure.

But I think, you know, the reason we're in the pickle we're in is because we have one number that we use for everything. And if we kind of decouple that from the

identity theft issues, it may go a long way to resolving this. But it would be a very difficult thing to do.

MS. DUNCAN: And I want to echo that. I think that one of the things that we tend to get ourselves wrapped up in is the whole what is identity theft issue, and we could debate that all day. But if you really focus in on the identifiers themselves that can cause the problems and then break that apart from what we would consider true just transactional fraud, they got my credit card and went off and bought the big screen TVs, and recognize where those risks are, then we need to start looking at how do we protect that number.

But I think adoption of 9 or 10 or 15 different industry numbers would be a huge, huge pushback from the consumer's standpoint. Probably all of us at the table.

MS. SINGH: Well, let's open it up to the audience for questions. We have the mics coming around the room. So, if you'll raise your hand and state your name and affiliation that would be great. Let's start in the back of the room there.

MR. BLAKLEY: Hi, Bob Blakley from the Burton Group. I wanted to ask all of those of you who have moved from Social Security numbers to your own internal identifiers whether you have yet had any experience of people attempting to steal those numbers in order to

commit fraud?

MR. DAVIS: Speaking from UCLA's perspective, we've had the UID in place for 15 years and the answer is no. We've not had any case on that. I mean, the real issue is what everyone is basically saying, is that it's -- even after 15 years, it's a very slow uptake, a very slow adoption, even though it's been pushed very hard.

MS. GRAY: And I'll speak from our perspective. No, we've not had that happen yet either, but we are cautious of that and cognizant of that. So, if someone loses their health insurance card, which has a unique identifier and not an SSN on it, in the beginning we thought we were just going to replace that card. No, we actually generate a new number just in case. It hasn't happened, knock on wood, but...

MR. SCHAUMANN: I think, too, it has to do with how you classify the number. Where we've seen it, the employee identifier, it's synonymous with your name, so it's basically a public piece of data. So, there's no value to it.

MS. GRAY: Yeah, there's not much you could do with it.

MR. SCHAUMANN: That's right.

MR. DAVIS: Right.

MR. SAKAMOTO-WENGEL: We have seen cases,

though, of identity theft involving medical record numbers where somebody will gain access to a medical record number and then use that to get healthcare using somebody else's name. So, that has occurred, as well as driver's license numbers where people used that to be able to purchase vehicles. So, there have been other means besides Social Security numbers of committing identity theft that we've seen.

UNIDENTIFIED MALE: Good morning, and thank you for the panel. My question is for Kim Duncan representing the banking industry. Quick question: How many tellers are there, do you have an estimate, in the United States and what safeguards have been put in place to protect them from them copying down the Social Security numbers that they'd have access to doing their job?

According to Mr. Webb in the first session, identity theft, maybe 50 percent of it comes from the workplace. So, I'm thinking you're very vulnerable in that area. How would you answer that?

MS. DUNCAN: I don't think we're any more vulnerable than anyone else in any other industry. As far as the number, I couldn't even take a guess. I mean, we're talking hundreds and hundreds and hundreds of thousands, if not millions, of bank employees. And the

risk, if you want to look at it that way, isn't limited to a bank teller. The risk is within every employee in every organization that stores this type of information. And it's incumbent upon us as employers to recognize what the need is for the use of that information, look at how we store that information, hence the internal identifiers, and then limit that information to those that have a need to know.

And, then, in addition to that, we have -- and without disclosing confidential information, many of us have internal processes that routinely scrub for use of inquiries to that type of information for those folks that may or may not need to have that information. You know, if somebody's sitting there doing 75 inquiries on client data in a three-minute period, that type of thing.

But I don't think the banks are any more vulnerable to that than anybody else is that stores that type of information.

MS. GIVENS: Thank you very much. Beth Givens, Privacy Rights Clearinghouse. I've been using just as a -- because, you know, we're all employees, employers, and we're all consumers. But a tactic that I've been using with some success is when I'm asked for my Social Security number, and I'll use my cable television company as an example, when you move to another part of the town,

you oftentimes have to get yourself at least a new cable television company. So, when I was asked for my Social Security number I said, I don't give that, how about my driver's license number? And they said, fine, we'll take that.

I wonder if you could comment on, say, a driver's license number being a useful substitute? It may not work -- like your case, as Jim Davis said, UCLA, but I'm thinking utilities and some other cable television, why not the driver's license number? We've certainly heard of enough insider thefts of Social Security numbers from utilities resulting in identity theft. Couldn't we use a driver's license number instead?

MR. SCHAUMANN: I recently had an experience where my wife was on a jury. And in that they went into this issue a little bit and it's actually quite astounding how much a large portion of the population don't have driver's license numbers, and if you don't have a driver's license number there is a state-issued ID number that you can get in the meantime. But, typically, mixing different data types in the same data field is not a good practice. There's a lot of risk for duplicates there.

MS. DUNCAN: And I would just also say that the

use of the driver's license can be just as problematic as the use of the SSN.

(Participant not at microphone)

MS. GIVENS: But it's not the key to the vast majority of (inaudible).

MS. DUNCAN: It may not be the key, but it is a key contributor. And when you look at the definition that the financial services industry uses for identity theft, you know, it's a combination of multiple things, one of which could be the driver's license number along with date of birth or Social or other individual personal identifiers. So, that driver's license can be very problematic as well.

(Participant not at microphone.)

UNIDENTIFIED FEMALE: Using it as an authenticator not (inaudible).

MS. DUNCAN: As her authenticator? I think you have to go back then to how is that driver's license issued. You're going to have a lot of discussion about that later on when we talk about authentication and how is the driver's license issuance authenticated.

MS. SINGH: We have an additional question up here.

MR. RUBIN: Thanks, hi, Joe Rubin with the Consumer Data Industry Association.

Question mostly for Mr. Davis. We've seen a lot of evidence over the last couple of years that data breaches generally do not lead to identity theft. I was wondering if you could talk about your experience with UCLA and how much of that breach did lead to actual identity theft. And then, secondarily, how difficult would it have been for you to identify alumni and other folks that you needed to notify without the use of Social Security numbers through Lexis or through other service providers?

MR. DAVIS: To the first question, I'm actually happy to report, but I say this cautiously, I'm happy to report that we've not been able to attribute any identity theft specifically to our particular breach. We have had a handful of cases that look like that and we will track that data down to some other database or some other breach.

I use the word "cautious," because as we heard this morning, people can sit on these for quite some time and, so, with one year into the breach, there's still a good possibility some of these could still pop up. I am keeping my fingers crossed.

The second question is the -- and I can't drill down too much in a lot of detail on this one because I simply don't know, but our alumni -- in other words,

finding lost alumni, you know, simply speaking, what the external affairs organization did was, we do have the advantage of having a rich record because these are past students. And, so, we can look at additional criteria besides the Social Security number.

And what they did do is work with these vendors that provide these services to look with others so that we are no longer collecting and storing the Social Security number or looking for it on that basis. And that's simply what was done, but it does depend upon the fact that we have a rich record of a past student and that gives us a large basis to ask a lot of other kinds of questions.

MS. SINGH: Back here.

MR. MASSEY: Hi, I'm a 27-year-old doctoral student at NC State which means that I'm in an interesting position with respect to my Social Security number. It's a nine-digit number that's been in use since 1935. Now January 1st, the Census Bureau said there were 300 million Americans alive today. These numbers are not reused, and sometime in the next 40 years or so, we're going to run out of Social Security numbers.

So, my question is, isn't it cheaper to transition to something different now than to wait 40 years when our legacy systems are even more embedded and

try to transition then?

MS. DUNCAN: That's an interesting concept, and I'll take that one. I would --

MS. GRAYSON: I'm with the Social Security Administration and I do Social Security number policy. So, I can address that question.

MS. DUNCAN: What did she say?

MS. GRAYSON: I'm Nancy Grayson, I'm with the Social Security Administration and I do Social Security number policy and we have issued about -- just under half of the numbers that are available within a nine-digit span right now. And as you say, eventually we will run out. But we are already looking at transitioning possibly to 10 digits. There's no consideration of reusing any numbers now because numbers are still used by people after they're dead for survivors and people that need to go back for financial reasons.

But the government usually fixes things when they have to and it will get fixed by then. So, I wouldn't worry too much about that.

And, also, I just wanted to say, along with what this group has been talking about, a lot of people are eligible for services, with businesses and all that are not eligible for Social Security numbers. So, chances are you already have something within your

validation systems or whatever, a way of telling someone's identity without a SSN, particularly like a lot of foreign students are no longer eligible for Social Security numbers, and a lot of people who are here that need services like gas and electric hookup and telephones, they are not going to get a Social Security number. So, if these companies want to continue to provide services, they're going to have to find another way to authenticate their identities already.

MS. SINGH: It's great to have someone from SSA to answer that.

MR. SAKAMOTO-WENGEL: One other -- I mean, also, I mean, technology is continuing to improve. And, I mean, it may not help with somebody calling in the middle of the night after their wallet's been stolen, but we may be moving towards biometrics in some situations and other means that we could have unique identifiers without using a Social Security number.

MS. DUNCAN: Yep, and I think that's the key. The use of the SSN is essential for the purpose that it's intended. In an industry like ours, it's tax reporting, it's regulatory requirements. But there are also other authentication issues that we have to deal with, who's calling in to our call center, who is in front of us to open an account, and utilizing the appropriate

authentication for that is crucial.

And, again, we'll have an authentication panel on later on, but at least from the financial services industry, our use of the Social is dictated, in most part, by what we have to do on the other end with that information. And I think that's the key to all of this, is look at the industry you're in, understand what it is that you're required to do and evaluate your need to use that number as either an authenticator or some type of an identifier.

MS. SINGH: Question here.

MR. HOOFNAGLE: Hi, this is a question that has to do with basically what the definition of "internal" is. So, to what extent are Social Security numbers used as an identifier or an authenticator in other countries by financial institutions or let's say, Bill, by your clients? Are they being transferred to other countries and used in those countries either for identification or authentication and what type of security safeguards are in place?

MR. SCHAUMANN: From a private sector, no. There's great pains taken to make sure it's not transferred and that's one of the challenges, if you have or try and go to a global -- for instance, a global HR system, you know, the EU rules and what you can move back

and forth apply there. So, SSN is primarily a U.S. problem.

A lot of times you'll see the field is government identifier and then the challenge is, well, in another country, what is the safe number to put into that field?

MS. SINGH: Question back here.

MR. KLOUDA: Tom Klouda from the Senate Finance Committee. And Jim sort of addressed this already, but I was curious if anybody is aware of where they actually went through the process of taking the SSNs out of the system, did it ever pose a problem in the future in terms of like a request from law enforcement or in a lawsuit you weren't able to match records? Was there some down side to the process that you went through to remove SSNs?

MR. SCHAUMANN: Well, I think -- I haven't heard of a situation where somebody has completely removed it. The idea is collect it once, secure it and use it only where you need to. So, I don't think you could ever remove it completely because you always need that binder to link it to whatever you're going to use in 90 percent of your transactions.

MS. GRAY: And I think that's what we were talking about when we talked about historical perspective, too. We still have it and use it for

internal reasons, so on and so forth. What we do is you have to back into it, there's a code that connects the UMI to the SSN for only those individuals within the company that have a need to get to that.

So, I agree with Bill, that getting rid of it completely is near on to impossible.

MS. SINGH: Question up here.

MS. OWENS: Good afternoon. My name is Barbara Owens and I work with Life Events Legal and also with Cole Background America. And I'm so happy to be here today in reference to learn exactly what you're actually going through.

I go around and I do the seminars in reference to affirmative defense response systems to companies and small companies on identity theft, and I'd like to ask you what is your take on educating and making what the Federal Trade Commissioners have put in place, actually we do that in compliance with what is going on and making the companies, the employees, the employers -- its just astounding how the employees and the employers react when they hear some of the stories that are going on. And we put them in response for their actions to be actually identified if they are not in compliance, if they don't follow the rules and regulations of the company and also someone in place.

Now, my question to you is: What is your take on the affirmative defense response system in educating the employees, the consumers and the employers on identity theft and what is actually taking place? I bet you a lot of these people here today are astonished in hearing what has actually happened in identity theft. So, the affirmative defense response system, what is your take on educating and making sure that it becomes a part of our responsibility as an employer or employee and be accountable to what is actually going on with your identity, and not only just changing the Social Security numbers because that is vast, but it can be done. It's a ritual, but it can be done. But what is your take on that?

MS. SINGH: I think we heard a little bit about sort of changing the corporate culture to think about that. And, Bill, I think you spoke on it.

MR. SCHAUMANN: From an education standpoint, it really becomes everybody's responsibility to make sure that, like I said, if you see SSN on a report someplace, you question how that's being used.

And I think one thing is we've heard a lot that people are reluctant to take a new number, but I have a kind of different opinion. I think people think it's a breath of fresh air that their company is taking the

steps to fix it and they will go along with it. So, I think education is key to a successful program, making sure that your employees know how it's supposed to be used and where and when.

MR. DAVIS: If I could jump in on this, too. First of all, I echo the importance of the education, it is absolutely vital. There are responsibilities by the individual that now need to be taken up.

I just wanted to elaborate a bit, and it was actually a point that Chris had made in the first panel. One of the things that has been, I think, particularly good with the notification laws is that it has raised a great deal of attention. So, if I look within our own university community the fact that these breaches or these incidents are being reported has raised a great deal of awareness. And then, certainly, the activity around a breach certainly increases the education awareness.

And I would say one of the things, with our own experience with a significant notification, was just the sheer awareness that was raised in credit reports and how to deal with credit reports and so forth, that was an important part that we were able to carry forward in a much stronger way.

MS. GRAY: I would just echo one thing Jim

said, which is that the breach awareness certainly does raise awareness. We have created a privacy department speaker's bureau at my company in which we go and we speak at staff meetings or whatever, whenever we're asked, and one of the hot topics and favorite topics is what we are doing not just about ID theft generally, but specifically medical ID theft. And we've gotten terrific response.

And much of what we're able to do is give examples of what has happened and, in fact, most persons in the audience have had that happen to them or know someone who does, and by that personalization that brings it home, too, and you treat everyone else's information as if it were own. That's our mantra. It's a change of corporate culture that comes after much of the education that you're talking about.

MS. SINGH: Question?

MR. DUNN: Hi, I'm Bill Dunn with the American Payroll Association. I have a question for Jim Davis. Unfortunately, I'm going to ask you to be the de facto representative for the entire university system.

This year, there were more than 40 data breaches by universities. And the one thing that I've been very curious about is that some of these breaches were lost laptops by professors or teaching assistants.

And I can understand all the administrative reasons why the university might need a Social Security number. I don't understand why a professor would need a Social Security number.

And it comes into something Bill Schaumann mentioned, the need to know, it seems to be a very basic tenet of security.

MR. DAVIS: I'll answer that and I also have my colleague, Rodney Peterson, over here, who is the EduCause security person and can speak across universities in general. But I can represent a fair swath of universities here on this one.

The faculty side of this thing is actually very, very important. First of all, that's one of the hardest groups to educate for starters. And, so, we actually spend a great deal of time. When we pick the faculty uses apart, though, there's a number of places that we're really trying to put some effort into. One have been things like reference letters. There are segments or disciplines in which they require Social Security numbers on reference letters. So, faculty tend to keep this stuff for years and years and, so, you can find this sort of thing on -- now, these tend to be onesie-twosie kinds of things, but, nevertheless, they are there.

The bigger issues have to do with the research side of things and, in particular, with medical information and patient information, and putting -- when one wants to work at home or when one wants to take their research data home, we have a number of situations which are we're really trying to reel in very, very tightly where faculty puts something on a thumb driver or on a laptop or this sort of thing, and that's where we have put in some pretty strong policies to basically restrict that happening whatsoever. But, nevertheless, that's where the educational piece comes in because we now need to have the faculty really take responsibility for this.

So, speaking for UCLA or the UC system, in general, there are a lot of policies that are in place now to deal with this, and it's really now an awareness and training kind of issue that we're really pushing very, very hard. But you're absolutely right, they should not have that kind of information on portable devices or deal with it unless it's a very, very specialized, known situation.

Rodney, I don't know if you have...

MS. SINGH: I think we have time for one more question. Okay, well, we can go ahead and break for lunch then. We need to be back here at 1:45 and we ask

that you all give yourselves enough time to get through security making your way back in, and please join me in thanking our panelists today.

(Applause.)

PANEL 3: SSN USE TO LINK DATA EXTERNALLY

MS. COHEN: Hello everyone and welcome back from lunch. I appreciate everyone coming back so promptly. We're just going to go ahead and get started with our third panel, SSN Use to Link Data Externally, and our moderator, Valerie Abend, the Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy at the U.S. Department of the Treasury.

MS. ABEND: Thank you very much and good afternoon. I heard you had a very productive first half of the morning today, so that was really good. I commend all of you for taking time out of your very busy schedules to devote to what is a very important subject matter here today, and I really appreciate the Federal Trade Commission hosting this event and bringing all of these great minds together to talk about this issue. It's a wonderful event to provide the appropriate lens and give all viewpoints in this kind of forum, I think it's very helpful.

So, thank you very much to my panelists for joining me today. I want you to know that we have a very good panel of experienced and knowledgeable resources here who are going to help us understand a little bit more, in plain language, hopefully, about how Social Security numbers are linked externally by their

organizations, how some of that may be impacted by various alternatives, if there are any alternatives, what might be the impacts of that, of using those alternatives.

And I'll tell you when I started to delve into this issue, particularly the external use issue, I was really struck by the amount of Social Security number solicitation and collection that's required by the federal, state and local governments. And, you know, that's obviously for a various number of reasons, including taxation and locating heirs, chasing down deadbeat patients, paying out insurance or other benefits, collecting debts, conducting background checks on employees, for example, and many other reasons. Some of these cases are, of course, driven by law, others are needed to assure accurate and timely and efficient secure financial transactions.

So, I'll tell you, obviously, the comments, if folks have seen the report that the FTC put together in advance of this workshop, have stressed how difficult it is to find an efficient alternative to use instead of the Social Security number for linking data externally and concerns that that would inevitably create some other type of vulnerable number or undercut existing security procedures and any fraud processes that are already in

place.

So, I did a little bit of research within just the Treasury Department to find out how we require or link Social Security numbers externally. And I was really struck by the number of examples just within the Treasury Department alone, and so, I want to talk a little bit about what I found and then, of course, turn to my panelists.

Obviously, the U.S. Department of the Treasury is not the only agency that does this with Social Security numbers or requires Social Security numbers, but we certainly are one of the key users of the SSN. Starting with the Internal Revenue Code which requires financial institutions to seek and obtain a tax identification number for taxation purposes, we call that a TIN, T-I-N. A TIN may be an employer identification number or an IRS issued individual taxpayer identification number, but for U.S. persons, it is the Social Security number.

So, I went and asked our tax policy folks to give me a short summary of IRS reporting requirements that must contain a Social Security number. The focus was on 1099s and 1098s, and I don't know why I was hoping for a short list, but the short list had 11 variations. So, on the 1099 for reporting of various sums of monies,

those include receipt of interest and dividends, proceeds from selling stocks or a real estate transaction, pension distributions, contributions to an IRA, student loan interest, insurance benefits, and payments to health savings account and then, obviously, more.

The Social Security number is exchanged between you, the individual, and the financial institution or between the financial institution and the IRS, but then when you think about it is that where really the number is just sort of exchanged between many of you, I know, myself, hire someone external to myself to compute and file my taxes so that obviously increases the number of individuals who are linking externally.

You have to ask yourself, does your financial institution use a separate entity to provide some of your financial services such as insurance, mortgage lending or brokerage, perhaps, and how do these entities make sure that they're accurately reporting to the IRS and accurately communicating with you about your assets and liabilities.

Turning to the enforcement side of Treasury, Treasury's Office of Terrorism and Financial Intelligence develops and implements U.S. government strategies to combat terrorist financing domestically and internationally, the National Money Laundering Strategy

and other policies and programs to fight financial crimes.

Financial institutions deal routinely with requirements to use a Social Security number under the Bank Secrecy Act as amended by the U.S. Patriot Act and with respect to requirements imposed by the Office of Foreign Asset Control or OFAC. For example, all customers for financial institutions are subject to what many of us refer to as the 326 Rule and that's the Section 326 of the U.S. Patriot Act. Financial institutions under this must have reasonable procedures for verifying the identity of persons opening a new account, maintaining records of verification information, and under the rule, U.S. persons must present a Social Security number when applying for an account with a financial institution.

Having a Social Security number also makes it easier for a financial institution to check against the OFAC list for prohibited persons and organizations because the OFAC list includes Social Security numbers, when available, of those targets.

Other examples are SAR reporting, what we call suspicious activity reports, and when they detect or suspect criminal activity in account transactions, financial institutions are required to submit this SAR

report, and those reports must include the Social Security number on the account holder if they have it.

Financial institutions must also report the Social Security numbers if they have it when filing what we call currency transaction reports or CTRs, to report payments of receipt for more than $10,000 in cash, an IRS Form 8300 filed by retailers when receiving more than $10,000 in currency for purchases of, for example, a car or jewelry or -- you know, have to report the Social Security number. So, any of you who are doing some pretty significant holiday shopping, you are now so forewarned.

There are just a few more examples with regard to public policy within the financial institution arena and I'm not going to delve into more than what I've already talked about, but suffice it to say, it's generally applied to identifying, verifying or matching information about a person or an organization.

So, with that, I'd like to introduce the distinguished panelists on my left. And they will talk individually and each of them will present briefly about their institution's uses and their organization's uses of Social Security numbers externally. And, then, then following that, I'll ask each of them a series of questions and then we'll open it up to the audience.

So, immediately to my left is Bob Ryan, the Vice President of TransUnion. On the phone with us, we have Stan Szwalbenest who is the Remote Channel Risk Director at JP Morgan Chase Consumer and Retail Franchise. Robbie Meyer is at the Vice President and Associate General Counsel of American Council of Life Insurers. Robert Townsend is member and past National Director of the National Association of Legal Investigators. Michael C. Lamb is Vice President and General Counsel at LexisNexis Risk and Information Analytics Group. And, then, Dr. Annie Anton is the Associate Professor of Software Engineering, North Carolina State University, Director of ThePrivacyPlace.org.

So, I'd like to begin with Bob Ryan.

MR. RYAN: Thank you, Valerie. TransUnion actually has many vice presidents, not as many as many banks, but quite a few. So, my actual role is Vice President for Government Relations for TransUnion. But I'm based in Chicago where the company is headquartered, I've been in the business many years, and although I spend a fair amount of time in Washington, I still call the corporate headquarters in Chicago home.

TransUnion, of course, is one of the three credit consumer reporting agencies in the United States.

We are also, increasingly, one of the providers of credit reporting services throughout the world. And, so, our experience of the issue of using a national identifier like Social Security number in other jurisdictions, in other parts of the world, our experience is global and so we -- and we can talk about this a little more later in the question sessions, but there are differences between -- that spring out of whether or not the identifying number is truly a national number and a robust national identifying system, as is true in some parts of Europe and South Africa and Hong Kong and elsewhere, or whether it is sort of an accidental identifier as is the case here in the United States or in Canada, or if a country has no real identifier at all. Someone earlier mentioned Brazil. Our experience in India is the same way. India has no national ID number, but they do have a tax number and a passport number, et cetera.

So, it does make a difference. And, so, that's why I'm so happy that the FTC is really delving into this issue, and it's a tremendously complicated issue to the respective roles of the sovereign state, whether that sovereign state is federal or state, read Real ID Act, and business in addressing the issues of how do you both identify individuals and, maximally, with greatest completeness and accuracy, run a credit reporting system

using an identifier like Social Security number.

From our perspective, I think it is not so much cost, although cost has come up at several points earlier in this symposium, as it is about accuracy and completeness. If we had access, for example, to driver's license number, which we don't, due in part to federal law which restricts the use of the driver's license number and the provision of it by the states. But if we did, or if we had access in the credit reporting system to a truly robust national database of cell phone numbers, for example, not calling information, but name, address and cell phone, if that accurate database actually existed, what a wonderful supplemental tool that could be for proper merging and authentication. But we don't, so we use what we have, which is this evolved system of the Social Security number.

Within the credit reporting system, there are four major ways in which we use the Social Security number to assure that we have as accurate and complete a credit reporting system as is possible. The first, perhaps most obvious, is not what you might think is the first, which is the production of credit reports, but the daily processing of millions of items of information, account updates, from all of the major and all of the minor financial institutions and other creditors in the

United States. We receive two to four billion updates every month on all of you and all of us up here who have credit accounts. That information is updated each month, and the vast majority, over 90 percent of that kind of information received directly from creditors, has the Social Security number.

In contrast, less than 20 percent of the public record, public record was brought up earlier and indeed it is important and indeed there are issues on it, but there are different practices within public record. For example, Social is apparently more available generally on marriage records or property records, but those are not particularly important or used by the credit reporting system. However, Social is not available in its full form on bankruptcy records due to the rule adopted by the Supreme Court and the U.S. courts a couple of years ago. It is also generally not present on civil judgments or releases of judgments or surprisingly on tax liens.

But the fact that it is very available on those four billion updates that we get each month is very important to the accuracy.

The second way in which we use it, as you would expect, is in the production of credit reports themselves. So, when you or I go and present ourselves and make an affirmative application for credit, of

course, we are almost always asked for a Social Security number. And although it is not always -- it's not required, but it is almost always provided, and that allows us to search our national file to bring forward all information that we might otherwise not have if you've changed your name recently due to a marriage or divorce, you've moved or had other informational changes that might not be reflected.

The third way in which a Social Security number's important is when we ourselves, you and I, exercise our rights under federal law and get a copy, go to the credit bureaus ourselves and want a disclosure of your TransUnion report. Again, it's not absolutely essential, but we will make you jump through some hoops if you don't want to give us that Social because, again, it assures that we're finding all of the information on you and making as complete a disclosure as we can.

And, finally, and just as important as the first three, Social Security number is very important when you dispute something, when you dispute the accuracy or completeness of your credit report and that, of course, triggers an obligation, a duty on the credit reporting agencies to go back to the original furnisher of the information and verify that. Well, part of our contact of them, or to them, will include your Social

Security number.

So, we think those are all important and it's all about being able to do that with a maximum amount of accuracy and completeness.

I think it's worth noting that although we use it in our data matching, we are smarter than to only use it in a black-and-white, on-or-off kind of nonjudgmental way that if we have a match on Social well, of course, then the data of course must match and we're going to merge the records.

Earlier someone talked about the unlawful immigrant problem and the fact and the reality that you can have a synthetic Social Security number that was adopted and being used very accurately, thank you very much, by 25 different unlawful immigrants, most of whom, by the way -- and to answer Joanna Crane's question about that dichotomy -- many of whom are probably paying their accounts just fine, thank you very much. They're good accounts, we just have 25 different folks using the same Social Security number.

So, my point there is that we're smart enough generally within our systems, and I'm not speaking for all of the credit reporting entities in the United States, but for myself and my own experience, to have algorithms that separate out and that apply some

judgment.

And I guess the final point I would make is that, again, in my company and I think generally this is true, we're certainly aware of this evolving issue as a public policy issue. There's been talk about the state laws. We, of course, have been very involved in the development or the negotiations, starting in California and through all the states, on restrictions of state laws. And, in general, we're fine. We're fine with California and we're fine with almost every other state.

We're about to begin -- for any of you who live in Minnesota, who read about Minnesota, mark your calendars for July 1st of 2008, Minnesota's going to adopt a new law which, unless the legislature changes it, will require the truncation of the Social Security number being returned in all credit reports, among other requirements. We're geared up and ready to do that. And the impact that will have will be something of a risk, it will be a real risk. Some systems are going to be, we fear, very adversely affected by that.

So, we're working -- and we will always work to comply with laws. We're working on alternative concepts, such as the ability to search for a file using a truncated Social Security number. We're very aware of -- I talked about it at the top of my remarks -- the idea of

additional, additional sources. And, again, I think part of our mantra is, this discussion, this discourse, we'd like to see be not so much about eliminating the use of Social Security number as about gaining, looking for more creative, additional paths like driver's license or like cell phone. That's where we are.

MS. ABEND: Thank you very much, Bob.

Turning to Stan Szwalbenest who is on the phone. Stan, are you with us?

MR. SZWALBENEST: Yes, I am.

MS. ABEND: We can hear you, so why don't you begin.

MR. SZWALBENEST: Great. So, Valerie, thank you for that great introduction you did earlier. Took a little bit of thunder about what I was going to discuss because what you were able to put your finger on is that from the -- and all I'm going to focus on is the external perspective, so how banks communicate with other parties and how we have to leverage the Social Security number.

Just for a little background for the folks in the room that don't know who Chase is, we're a little community bank based out of New York. We have $1.5 trillion in assets, we operate in 50 countries. Within the United States, our footprint consists of 17 states, around 3,000 branches and 8,500 ATMs.

As Valerie pointed out, I'm the Remote Channel Risk Director, that covers basically anything that's not the brick-and-mortar branch. I help set some strategy related to anything from authentication down to some real security issues and concerns.

With respect to how we communicate with third-party servicers, I kind of broke this out into several chunks. The first is third-party servicers and then the latter is going to be government agencies. From a third-party servicer perspective, the credit process, especially in this environment, is essential for us to get solid credit reporting. So, our interaction using the Social is how we report back to the credit agencies. The previous speaker discussed there's billions of transactions a month that are provided on the credit side.

We also use the same Socials when, you know, not only in the new account screening process for these credit products, but also on the performance side and how we report out how credit is performing and even how deposit accounts perform. So, there's an interaction with credit agencies in those aspects. I think those are the more well-known uses.

Some less well-known uses would be how we authenticate and comply with the Patriot Act. We use the

same information to communicate with credit agencies to get knowledge-based authentication questions. We use the same sort of information to communicate with non-credit agencies, such as vendors that aggregate data, similar like LexisNexis and a number of other providers, to collect other kinds of questions, even public record aggregation, so that we can better authenticate who we're dealing with. Because, you know, Social Security numbers are so widely used, banks can't really rely on that as an authentication question or device. So, it's really just a cuing device or an identification device.

We talked about the credit process, we talked about new account screening, and we talked about authentication into our firm. On the flip side, we also use it for communicating to government agencies, right from the employee aspect, how we report earnings, to customer revenue, how much customers are earning on their various accounts on instruments back to the IRS. We use it when we communicate with law enforcement around suspicious transactions, suspicious behaviors. We have to include it in all of our OFAC notifications, and I can run down a laundry list.

We also use it for beneficial things. Helping identify during disaster relief, when we have to provide funds. So, it's heavily used when the bank is

communicating to third party agencies, for no other reason than for being able to identify the record.

And as the previous speaker pointed out, it's not just the Social. Because, again, it is heavily used. There are keying errors. So, it's the Social in addition to other factors like an address or the full name. So, we provide multiple pieces of information which then go through some sort of logic to help identify those accounts at other agencies.

MS. ABEND: Thank you, Stan. And turning to Robbie.

MS. MEYER: Thank you, nice to be here. I'm Robbie Meyer of the ACLI. The ACLI, the American Council of Life Insurers, is the principal trade association for life insurance companies in the United States. Life insurers, as you would imagine, are very much committed to combating identity theft, have developed very robust security procedures long before Gramm-Leach-Bliley was enacted and, certainly, after the enactment of Gramm-Leach-Bliley. But, also, as you know, and as Valerie and Stan said, there are numerous federal, state and local laws applicable to life insurers that will require them to collect Social Security numbers and to use them in various reports and to use them in a host of other ways in order to meet the requirement of these laws.

And because of the fact that there are these governmental requirements that are essential on all levels of government, coupled with the fact that the numbers really are the most effective identifier, and in our view, the numbers have become intrinsically tied to many of our activities, both our identification activities, our internal ID activities, as well as our external identification activities that I'm going to focus on now, as well as our authentication procedures.

And by virtue of the fact that the Social Security numbers are universal and they're unique and they don't change over time, they are particularly important to our member company life insurers that issue contracts that are likely to be enforced for 10, 20, 30, 40 years, that actually cover individuals from cradle to grave. Also, given the fact that we gather not just financial information but medical information, there's heightened sensitivity and concern about the way in which we maintain both the privacy and the security of that information and real concern about the fact that the reports that we obtain, we maintain and we disclose to others are accurate when we are using them.

And as I looked at the list of ways in which our member company life insurers use Social Security numbers in preparing for this presentation, I was really

struck by the many ways in which companies actually do use them to externally link in order to be sure that we are either getting the correct information or to verify information that we obtain and also in order to make sure, again, that the information that we're obtaining, maintaining or sharing with others is accurate.

And just as both Valerie and Stan said, there are a host of legal requirements, reporting requirements, requirements to protect against anti-terrorism, or terrorism, money laundering, fraud, there are a host of state and federal laws that require external linking in a number of ways. We have to, again, report income, interest, dividends and benefits in connection with a number of our products to both federal, state and local entities. We include the Social Security numbers in those reports, to be sure that we're reporting and the information is associated with the correct individual, again, in connection with the Bank Secrecy Act itself that requires all insurers have any money-laundering laws; in connection with the U.S. Patriot Act Amendments, to the Bank Secrecy Act that impose additional know your customer obligations.

We use Social Security numbers in order to connect with external third-party databases to be sure that we indeed know the individual with whom we're doing

business. Again, just as Valerie said, in connection with reports regarding suspicious activity, transactions over $10,000, again, life insurers like other financial institutions use the numbers to be sure that those reports are, again, associated with the right individual.

We also use the numbers to comply with federal law that says insurance companies can't hire individuals and have employees who are convicted of felonies, that are engaged in dishonest activity. Again, use the numbers to review criminal databases and criminal reports, again, to be sure that in fact, we are getting information about the correct individual.

On the state level, there are a number of other state laws that either mandate, again, mandate our use of the numbers or we have to use those numbers in order to fulfill those obligations. Social Security numbers are used in connection with state escheat laws, when we're reporting unclaimed property, we use Social Security numbers in connection with state laws that prohibit payment of claims until we check to be sure that an individual or a claimant is not on a deadbeat parent list or is delinquent in paying their state taxes. We use them in biographical affidavits on our executives and officers that we're required to file with state insurance departments.

In connection with long-term care partnership programs, the Social Security number is the primary identifier that is used by companies that are reporting to the states that are engaged in these partnership programs. The Deficit Reduction Act that was just effective in 2006 expanded the long-term care partnership programs to all the states, as I understand it. Again, we'll be creating another database of information about long-term care partnership policies that individuals own in states across the country.

Again, the Social Security number is the primary identifier to be sure that all the information about all those long-term care policies participating in the program are identified with the correct individual. Very critically and maybe unique to the insurance industry, Social Security numbers are used to make sure that we get the right medical records on individuals who apply to us for new coverage, who submit claims under existing policies. It's our understanding that many healthcare providers are very concerned about disclosing health records without having a Social Security number. They're worried about it and we're worried about it, too, as our customers, again, to be sure that we're getting the records of the correct individual.

Use the numbers to administer retirement plans

and our communications between a life insurer that's administering a plan and our employer customers to make sure, again, that the information that we receive is credited to or associated with the correct individual. We use, again, the numbers to perform basic background checks. We use the numbers in connection with disability income policies and our communications with the Social Security Administration, to make sure that there has not been a duplication of payments, a duplication of payment of benefits so that a disability income insurer does not pay benefits that have already been paid out by the Social Security Administration.

We also use the numbers across our holding companies, where we have a life insurer that's part of a financial services holding company that comprises a bank, a securities firm. We use the numbers to make sure that we are helping individuals locate accounts or policies for which they've forgotten the numbers. We also use them to be sure that when there's a transfer from one type of account, from an insurance policy, from an annuity to a bank account to a security account, that we are making sure the monies goes to the correct account or the correct individual.

So the bottom line in our world is, is that these numbers are intrinsically tied to our systems and

they are so very important, particularly in the context of this external linking, because they are the one universal number that does not change over an individual's lifetime. Thank you.

MS. ABEND: Thank you, Robbie. Turning to Robert Townsend.

MR. TOWNSEND: Thank you, Madam Chairman. I want to thank our government and members of the FTC that arranged this workshop and invited my participation. I look forward to the exchange of ideas and viewpoints and creative thinking that will resolve this problem in the best interest for John Q. Public, the consumer, of which I'm one. Although I'm a licensed legal professional investigator, I am just as subject to identity theft and the adverse consequences from that as you are and as any other American citizen is.

I have been a licensed professional investigator for 47 years. That's the better part of my lifetime. It's been good to me. It's been good to me because I have been good to it and the people I serve. Any licensed legal professional investigator will have the same reaction that I have, you get what you give.

My comments today do not represent any particular association. They are my views and my views alone. But they're from the street. They're from the

day-to-day knock-around obtaining information on particular issues about particular people under a particular set of given circumstances. And ladies and gentlemen, that's key. Under a particular set of given circumstances.

Ask yourself what professional is going to expend the time, the money, the effort, the intellectual capability to willy-nilly go out, obtain Social Security numbers, and use them to perform identity theft. It does not happen. Also ask yourselves what motivates a licensed legal professional investigator to obtain a Social Security number. He's being paid to obtain that information and to link, with clarity, all information associated with that Social Security number.

Now, when there are so-called investigators that step over the line, they're usually held out as examples of the private investigator. In most cases that's simply not true and it seems to be the case in the most recent exposures in our great Northwest. But, more importantly, what motivated the investigators to do what they did or to attempt to do what they did? It was dollars.

Some client instructed that investigator or those investigators to go and do. In exchange, they would render a statement for services. That statement

for services was to be paid either prior to or after the fact.

So, when there's a penalty, when there is jail time, when there is a loss of license, don't limit it to the investigator that's out there stepping over the line. Have it go back up the chain to the benefactor of that information. And, believe me, you'll stop it dead in its tracks. You really will.

For a private investigator, licensed and legal, a member of national associations, educated, up to date on the day-to-day law and how it works, immediate access to a unique personal identifier, such as a Social Security number, is absolute. We locate missing witnesses, heirs, missing children. You name it, we do it, and we do it and sort it out by linkage with an SSN. In some cases when there are races involved, the SSN is the only unique personal identifier to distinguish one John Jones from the other hundred John Joneses in the area.

Now, if I'm out conducting a pre-litigation investigation, you, Mr. John Jones, do not want to be the John Jones that I focus on as the person responsible for the wrongdoing I'm following up on if you're not that John Jones. And the best way to preclude that is to give me continued access to the Social Security number.

Now, how can you do that and be assured that it's not going to be misused? Confine immediate access to licensed legal professional investigators, require that they have a continuing liability policy in substantial amounts similar to one million/three million, on liability issues alone, particularly a special endorsement in that amount for access to Social Security numbers.

When that insurance expires, notification goes to the regulatory authority that that insurance has expired which, in turn, goes to the database providers which, in turn, discontinues doing business with that particular investigator until he can provide adequate insurance. Because when you're out on surveillance and you have a cluster of vehicles and you have a cluster of people, you have to be able to distinguish one from the other and, believe me, I have been in situations where there have been three or four John Joneses, all within the same general age groups.

The Social Security number is mandatory, you want it to be mandatory. You don't want to be the wrong John Jones when I'm out there looking at you. That's one suggestion insofar as the Social Security number is concerned.

Another is what I call, for the sake of a

better term of prose, is a master system. There is absolutely no reason that I, as a licensed professional investigator, should have unfettered access to your private information. I don't want you to have unfettered access to my private information. But let's say we're involved in some business relationship that has gone south, we've been involved in an accident involving extensive personal injuries, I've consulted an attorney, and the attorney has a need to determine if there is any viability for his litigation. With that, he provides an assignment and an affidavit that he is entertaining litigation against a particular individual.

I, the investigator, go to a retired justice active within the justice system or a sitting justice within the justice system, be it federal jurisdiction or be it state jurisdiction. I pay the fee, it should be self-sustaining on the fee. I provide my ex parte argument. The judge grants me the authority to obtain limited information to determine if a lawsuit is required, and if a lawsuit is required, that the end result can end in compensation for the injured or damaged party. That warrant essentially is a civil search warrant, a restricted civil search warrant to be sure.

Now, let's take it a step further. What happens if litigation goes forward and I need to dig

further in-depth? I need to determine your assets. I need to determine the names of other members of your family. I need to determine their assets to trace funds. Do you not want me to have a judicial set of eyes looking at what I'm doing, telling me what I'm doing is sanctioned?

There are many more ideas beyond my expert techniques. We have a room full of investigators, association representatives here today, that can answer questions that I might not be able to. Thank you for this opportunity.

MS. ABEND: Thank you, Robert. And, now, to Michael Lamb.

MR. LAMB: Thank you, Valerie, and I'd like to thank the FTC for allowing LexisNexis to participate in the workshop because we absolutely agree that the impact on consumers of using Social Security numbers in data linking is extremely important. It's not just for industry and how well our systems work, it's really important for consumers themselves.

Before I go into data linking and algorithms and eyes start to glaze over a little bit, I want to step back a little bit and try a little bit of just context on my perspective on identity theft and information. I believe that information is not the problem when it comes

to fighting identity theft and Social Security numbers are not the problem. Instead, I think information is the solution for fighting identity theft. The bad guys, a fraudster can only really succeed if he or she knows more about a person than the business or the financial institution that's being defrauded knows about that person.

As we step back, and particularly in today's technology age, despite the best efforts of consumers and businesses and the Commission, the data thieves will always exist and they're going to be attacking computers and mailboxes and purses and wallets, and we've heard about ways they get the data. And I believe the key and the real focus needs to be on making it very difficult for them to use that information because someone's always going to get it, and we need to give consumers and businesses and financial institutions better weapons and better information than the bad guys have, and that's the key business LexisNexis is in and Social Security numbers are part of that business.

You know, we create, among other things, anti-fraud, anti-identity authentication tools, and it's by using those tools and making them easy to use that we can really stop identity theft because mailboxes are always going to be there, purses are always going to be there.

And we've heard this morning a number of ways that people obtain data.

Now, to step back a little bit and actually talk about what LexisNexis does and how we link data, a lot of people in this room know about our services. I think probably almost every panel member has probably either used them or might use them, ranging from universities to law enforcement to the financial institutions. We collect data from the various public and private sources and we link that data in our database to specific consumer identities. We collect from, I think, 9,000 different public record sources alone and we collect from private record sources. It's real estate records, court judgments, liens, bankruptcies, telephone numbers, addresses, alternative names.

And then we have linking algorithms that take that data -- and we have, I think, over seven billion records on consumers and total number of sources is about 35,000 sources. And we take that data, and the key is to make it not just data, we don't make data available to people, we make services available to people.

I think it was Stan who might have talked about how they do additional authentication when somebody wants to call in to change the address for their checking or credit card account, and we create services where you ask

so-called out-of-wallet questions. Even though it's the bank talking to their own customer, they'll ask a question somebody who stole that customer's wallet wouldn't know. Which of the following three states did you used to live in or which of the following three cars did you used to own? Trying to make it simple for consumers, but effective, you know, this sort of knowledge-based authentication.

It's great to have a special ID number, but people don't know those ID numbers and they might have to dig them out of their own computers. But they know the kind of information that -- and this is what call centers need, something the bad guys won't have. We need to arm people with these tools and we hope these firms meet their know your customers obligations and anti-money laundering obligations, and we have to do it a real, cost-effective, immediate way. You can't say I'll get back to you in three days after investigating whether you are who you say you are.

Finally, the same tools and databases are used to fight terrorism and crime. We serve federal and state law enforcement as well as a number of federal agencies, and again, trying to locate people, trace identities, see relationships between the identities. It's by using the data and using the links among them that you can put

together effective services.

Now, to step back and say how do we use Social Security numbers in that context. We have a super computer center down in Boca Raton, Florida, which is probably one of the biggest super computers on the East Coast and we receive the data and we have rule sets and algorithms that link it to specific identities. I went to our technical people and they said we have over 100,000 algorithms and rule sets. And they're designed to link data including Social Security numbers, which is a very important data point, but it's only one among many, and you have to go through algorithms to say have we seen data in the same combination from other sources. That's an indication that it's accurate data.

We have rule sets designed to address mis-keyed Social Security numbers. There's often one or two digits that are off. But if you see it off, but you see a consistency elsewhere then you can automatically correct Social Security numbers.

We deal with multiple Social Security numbers. As we've seen, they come into the system, either people misusing a Social Security, making one up comes into a context, and we have to try to then create a set of data that's associated with a specific identity. You know, names change over time, and the Social Security number is

the one data point that persists and it's unique. Name, address, telephone number will all change and change constantly.

And that's why, even though you don't link solely based on Social Security number, it gives you a name and typically you're getting it in a context where it's a name, an address and a phone number from a reliable source and then you can build upon that with the tax records, the criminal records, the real estate records that may not have a Social themselves, but the Social is one of the foundations you build upon.

I know people have talked about alternatives and can we just use partial Social Security numbers. So, I went and pulled some data from our system. We have over 15,000 identities in the U.S. that are some variation on Will Johnson. Not John Smith, I didn't want to quite go to that extreme. But you have William, Bill, Will, Willard, they're all a variation on Will Johnson. And if you just have the last four digits of the Social Security number to differentiate those Will Johnsons from each other, I asked how many of those Will Johnsons share the last four digits with at least one other Will Johnson, and it's over 4,000 Will Johnsons share the last four digits with another Will Johnson. And I have almost 10 where the last four digits are common among at least

seven people.

And at some level, you know, yes, it's a decrease in accuracy, is that the end of the world if we protect Social Security numbers, I think it truly is a significant impact. If you're somebody who's applying for credit or who's applying for a job and you have criminal records associated with you from some other Will Johnson, you want the system to be as accurate as it can be within reason.

So, yes, a decrease in accuracy, even if it maybe goes from 99 percent to 90, whatever it may be, that's an extremely significant decrease. And to step back and say what's the consumer impact, we've talked a lot about the impact on the businesses. I think with the consumers, if they were to know that by taking away a full Social from these kind of linking uses that are anti-fraud tools and wouldn't work quite as well, and you might have to explain some criminal records that weren't theirs, you know, more than likely -- and, yes, they have the right to do that under the FCRA. There are rules in place. But why go through that if we're going to have accurate linking?

I look at the Minnesota law that Bob Ryan mentioned, and I'm very concerned about the Minnesota law if it's not changed, where we will no longer get full

Social Security numbers on people from Minnesota. And as a result, our anti-fraud services will not work as well there, collections efforts won't be as accurately targeted there, people may be getting collections from the wrong Will Johnson in that case. There are consumer impacts from taking away things like Social Security numbers.

If you look at the real harm of identity theft, usually the loss is borne by the credit card company, but the harm is the confusion in straightening out your record. By taking away the Social Security number, you're imposing that harm without even the intervention of an identity theft. You're creating the harm through the confusion in the system itself.

Now, I want to talk about a few examples that go beyond just credit and credit cards and finance and banks, because if you impose rules on Social Security numbers, it's going to spill over into the other types of data linking that the companies do. One of our customers helps find the beneficiaries for pension funds. They use Social Security numbers, they give them to us, they track down the beneficiaries of the pension fund. They couldn't do that nearly as accurately without Social Security numbers.

Our data is used to help track down

unregistered sex offenders. Our data was used, I think, in 2006 to help recover 146 missing children. Those are the kind of things where is a decrease in accuracy acceptable, and I think the answer to us is no, and I think most consumers would frankly agree with that.

To step back to sort of what I said at the beginning, information is the solution and we can best fight identity theft if we make sure the good guys have better information than the bad guys. And, you know, as we work with banks and law enforcement and the other people trying to use identities, the consumer harm from decreasing the accuracy of linking by restricting the use of Social Security numbers would, in my opinion, far outweigh the potential benefits. Thank you.

MS. ABEND: Thank you, Michael. Now, I'd like to turn to Dr. Anton who is going to give us a little bit of a different perspective with regards to possible alternatives.

DR. ANTON: Thank you for the opportunity to speak today. As previously mentioned I'm a Associate Professor of Software Engineering at North Carolina State University, and I'm the Director of an academic privacy research center named ThePrivacyPlace. In addition, I serve on several industry and government boards including the DHS Data Privacy and Integrity Advisory Committee.

So, right now, personal information about you, me and millions of Americans is being compiled, accessed, sold and exchanged among businesses and government agencies. Yet, we should all be concerned. Is that personal information protected? Is it correct? Is it being shared among those with a legitimate need for it? Is it being used for legitimate purposes? And can criminals easily access our personal information?

These concerns are compounded by three factors. First, the widespread use of Social Security numbers has made it into a de facto national identification number. Second, computing technologies enable us to collect, exchange and analyze personal information on an unprecedented scale. And, third, there are widespread problems with cyber security leading to frequent large security breaches. In particular, technology allows personal information to be combined with Social Security numbers, thus creating a convenient way to track individuals' public and private records. This raises privacy concerns and these concerns are exacerbated because businesses use the Social Security number as both an identifier and a authenticator.

The terms "identifier" and "authenticator" have very specific technical meanings that are often confused. An identifier is a label associated with a person. An

authenticator provides a basis to believe that somebody is accurately labeled by that identifier. Authenticators might be something you know such as a secret password or your PIN, something you have like the key to your house, or something you are, such as a biometric. A Social Security number is an identifier. It is something that anyone can know and many will. So, it's not a secret. Hence, it is unusable as an authenticator, though many organizations use it that way, and this is a big problem.

My passport picture coupled with a tamper evidence security seal is an authenticator because it links me using something I am as embodied by my photograph with my identity. Using Social Security numbers for both identification and authentication makes them much more valuable to a criminal who is intent on stealing someone's identity. This is a problem of our own making and it is a problem that we can eliminate.

In the remaining time, I'll provide a few recommendations. First, we should move away from authentication based on information that is easily compromised. Social Security numbers and mother's maiden names are poor choices for authentication.

Second, if organizations are going to continue to use the Social Security number as an identifier then everyone should be able to publish their Social Security

number without concern about what might happen to their accounts. Moreover, organizations and companies, not consumers, should be held responsible for any loss to consumers who become victims of identity theft caused by continued reliance on the Social Security number or other readily available information as authenticators; in other words, a private right of action for consumers and legal liability for organizations' business practices.

Third, we should require stronger security practices during the transmission and storage of Social Security numbers and all other personal information.

Finally, I was asked to comment on whether there are alternative identifiers or data points that can work as effectively as a Social Security number for data-matching purposes. Databases containing personal information often employ the Social Security number as the primary key or common identifier. This presents yet another vulnerability making it easy to match records from disparate data sources.

Replacing Social Security numbers is not a large technical hurdle. We can better protect individual privacy using different random numbers in each company database. This would prevent someone from easily correlating the personal data about an individual in several of those databases. The Social Security number

can still be used to link data externally, however, by simply keeping a separate secure database of Social Security numbers that is indexed with the internal company ID numbers. Then, when a transfer of data occurs or data needs to be linked externally, an additional database look-up is performed to map the company-generated identifiers with the appropriate Social Security numbers.

The total cost of processing is minimal, as this would only require one extra database look-up. And, more importantly, this limits the risk of exposure.

In conclusion, the Federal Trade Commission has a strong track record of protecting the privacy and identities of U.S. citizens. I'm encouraged by the attention to these issues and I stand ready to help in your efforts. Thank you.

MS. ABEND: Well, thank you all very much for your opening remarks. I think we have a lot of different perspectives here, and not necessarily full agreement, which is a good thing, because then it encourages really good open debate and I appreciate that.

So, I want to start out just asking some questions of the folks on the panel. A number of you touched upon the issue of the Social Security number not being the only number that your organization uses to

identify or authenticate individuals in your databases for various purposes, particularly Robert from TransUnion, as well as Stan from JP and Michael from LexisNexis. And I was curious about the fact that it's not the only number that's used and I was interested if you weigh in some way the Social Security number as the identifier versus some of the other factors so that some are more reliable, others aren't, and you weight them in some way as you try and figure out whether this person is that person or not and you're doing this external linking.

So, I'll start with you, Robert, if you don't mind.

MR. RYAN: Okay, thank you. The short answer is, yes, we do. The weightings are very complicated and, of course, proprietary. I think I would also, though -- and I can get to that in a little bit, but I must comment that, in fact, the process that we use today and that has been in use for years to update those four billion account updates every month from financial institutions is actually precisely what Dr. Anton described in a sense that we are receiving from Chase, for example, their data sets of their various accounts, their Mastercards and Visas, their auto loans, their mortgages, et cetera, and that data includes the Social Security number, yes, but

it also includes -- and, in fact, the primary match key for us is the self-generated account number by Chase, which is unique to Chase, proprietary to Chase.

And, so, the actual transactional flow is that, you know, we get those data sets in and tens of thousands or millions of records from -- I'm sorry, Stan, but I'm picking on Chase, but this is true for everybody.

MR. SZWALBENEST: That's okay.

MR. RYAN: So, anyway, I think that's important to note or to think about, that we are actually using that, a combination of SSN but, in fact, where the primary key is the account number generated from Chase.

To your question, I can't get into the details, but, sure, there are all sorts of very complicated algorithms that say, yes, well, these two possible records, one is a junior and one has no suffix and the Socials are, well, they're the same or, gosh, there's a transposition position, or what do we know about the age in which that Social -- we know about the month and year or the state and age issuance. So, it's very complicated, and yes, algorithms are used to make those kinds of decisions.

MS. ABEND: I suppose the reason why I'm asking this question is because as we think about Social Security numbers and some have talked about the

pervasiveness of the use of Social Security numbers and the concerns about identity theft, that to the extent that the value of the Social Security number itself presents not necessarily a universal value amongst various institutions, if you will, and not -- it doesn't have, necessarily, the same value tied to it as we once thought it may, so that it's not the key that opens the door for all services in all cases.

I'm trying to get an understanding a little bit of that, I think would be helpful for the audience. So, Stan, do you have any more comments on that?

MR. SZWALBENEST: Absolutely. So, I think the best way of putting it is there was a time where the Social was the key to the kingdom, but that time has long passed, maybe 20 years. It's used as an element, as an identifier. Because we use so many different tools and we even use information within our own walls to help authenticate, so we have identifiers, but it still doesn't authenticate.

So, Valerie, I'll pick on you. So, you could call the bank and we can say give us your last four digits of your Social, but that doesn't do anything other than -- that combined with your account number helps us find you in our files and then we will ask you the questions about transactions or where you live or what

color your car might have been in 1989. So, using any number of different third-party servicers, as well as what we have within our own company.

So, on its own, it doesn't do anything other than it's a key within our own brick-and-mortar, and then as we communicate outside the company, as the gentleman from TransUnion said, it's one of the elements used to identify and so on, due to the complex algorithms they use.

MS. ABEND: Thank you. And, Michael, do you have anything?

MR. LAMB: No, I absolutely agree. And not only is a Social Security number just one data point to use as a identifier in your formulas, but the circumstances under which you obtained it. If you obtain a Social Security number in credit header data, there's a great deal of reliability in that. If it's in a criminal record, which is usually filled out by the criminal him or herself as opposed to the driver's license number, it has no reliability usually because it's usually made up.

DR. ANTON: So, I'm curious about this statement that Social Security numbers are no longer the key, they used to be, because the figures I keep seeing are that, gosh, they're being used a lot and they are the key and this is the major problem that we have in

identity theft. And, so, if they are no longer the key, why do we continue to have identity theft?

MS. ABEND: Go ahead, Robbie.

MS. MEYER: Well, I think when you're talking about this external linking, there's a particular issue here because the numbers are a universal number that is used by government and by business. And when you're using commercial databases to perform criminal checks or background checks, the fact is that the number continues to be the key number, or I'm told the primary identifier with these state long-term care partnership programs or communicating with the Social Security Administration.

I think that in connection with these external linkages because they are a universal that does not change, they are critical. At the same time, I know that financial institutions, like life insurers, are subject to these very stringent obligations under state and federal law to maintain the security of the information themselves and then the entities to which they disclose them are subject to the security obligations. And, so, I think that there are checks there.

But I think that when you're talking about external linking, because they are the universal, until they stop being this universal number, I think they are critical to the external linking, but I think that

security is maintained in most cases. I can't say that it's guaranteed across the board, but in most cases, particularly in the context of financial institutions and life insurance companies.

MR. LAMB: Could I add just one thing? They are a very, very important identifier. They should not be used as an authenticator. Name and Social Security number together should not get somebody a credit card. We've moved beyond that. The bad guys are too good. The tools that are available for authentication are more sophisticated than that.

But is it a critical identifier, critical to pass information from one organization to another? Absolutely, yes.

DR. ANTON: I'd like to add that asking for the last four digits of a Social is even worse than asking for the entire social.

MR. TOWNSEND: May I jump in here as well? I'd like to piggyback to the Doctor's excellent question by saying, if the Social Security number is not the primary identifier in linkage how is it so many private investigators are accused of performing identity theft with the use of the Social Security number? And let me continue that further, how is it that we in the private investigative profession need the -- I'm sorry, that we

continue to be restricted from access to a complete Social Security number if it's not the primary source for identity theft?

MS. ABEND: Very important questions. I want to ask the panel one more question before we go on to the audience and we're a little bit crunched for time, so I want to make sure I get this one other issue on the table and that is the issue of security.

I know, Robbie, you mentioned that security, because you have both health and financial information on the table when you're dealing with clients, when your members are dealing with clients. So, I wonder if you could talk a little bit more about the safeguards, best practices maybe that members of your organization use with regards to securing that kind of information when they're doing external linkages. And then, following that, I think let's go to the audience.

MS. MEYER: Thank you. I think there is a particular concern in dealing with medical information. Consumers are understandably very concerned about that, so that our member companies and life insurers in general are subject to a host of -- the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, and then a host of different state laws that implement the Gramm-Leach-Bliley obligations as well as old privacy laws that insurers

have been subject to over the years, the understanding being that if our customers are worried about giving us their most sensitive information, they're going to talk with their feet.

So, there is a real understanding and appreciation of the fact that it is absolutely imperative that we keep it secure so that we adhere to the administrative, technical and physical safeguards obligations that are required under the Gramm-Leach-Bliley Act. Individual companies have their own techniques, their own specific barriers for heightened levels of protection, security protections, and physical protections for that information that they retain on premises, that they operate on a need-to-know, need-to-use type premises, or a technique.

However, they are very, very -- I would say that most of their protections are governed by the host of federal and state laws out there that require very specific obligations with respect to both the security of the information as well as the circumstances under which the information can be disclosed to affiliates or non-affiliated third parties.

MS. ABEND: So, from your perspective, it's both a combination of the legal requirements as well as the reputational risk that sort of govern the motivation

behind what activities they're doing?

MS. MEYER: Absolutely.

MS. ABEND: So, I don't want to take away from the audience time, why don't we answer some questions that are available.

MS. BOCRA: Hi, my name is Nicole Bocra, and I am a private investigator here in Virginia and I'm also registered up in New Jersey. I own my business, I've been in business two and a half years now, and I'm the type of person you want to have access to that information.

I conduct mortgage fraud investigations, so far I've done 19 in 2007. When the banks had trouble with all the sub-prime stuff they had me, you know, interviewing neighbors and figuring out who used to live there. The only way to do that is based on the Social Security numbers to find witnesses.

I specialize in stock market fraud and locating assets, that's what I do for a living. When it comes to it, I'm subject to state and federal regulations. I'm subject to be audited. I have a bond, a significant bond that I pay in two states. My insurance is astronomical. And the bottom line is you really won't know that you need a private investigator or you need access to that information until something happens to you, until you're

in a motor vehicle accident and you want to speak to those witnesses. And if you have three witnesses and they all have very common names, how do I find them?

So what I'd like to say is I'd like the FTC and everyone else to keep in mind that I need access to that information for a permissible reason, similar to the Drivers Privacy Protection Act where I need a exemption to use it.

So, my comments are I'd like to thank everyone for participating and I'd like you to keep in mind that Social Security numbers are necessary for what we do. Thank you.

MS. ABEND: The gentleman over here.

MR. BLAKLEY: Hi, Bob Blakley from Burton Group again. I just want to maybe try and draw out a little bit more nuanced response to Annie Anton's question about the use of Social Security numbers to perform identity fraud.

The panel seemed to indicate that, for example, knowledge-based authentication or an equally mature authentication process is used by all institutions for all transactions and that, therefore, Social Security numbers are no longer the keys to the kingdom. I think that oversimplifies matters along two different axes.

It is certainly the case that new account

protections are much better than they used to be, but there's still lots of transactions, including small value transactions and transactions such as changing the address to which a statement is sent, which are authenticated much less strongly, sometimes just with the last four digits of the Social Security number. When you combine that with the fact that identity thieves are at least as smart as the people in this room and know that they can get a Social Security number and use, for example, a fraudulent credential as a private investigator or some other method of access, pretexting and so forth, to get additional information before they initiate an identity fraud attempt, you still have a lot of ways into the identity fortress.

And I think that it is these chains of access and, also, the perception that some of the identity transactions are low value and, therefore, not worth protecting with the stronger methods of authentication that we are seeing the results of these days and I'd like to have comments from the panel on that.

MR. SZWALBENEST: I'd like to take that one just out of the gate. The manner in which FIs authenticate consumers varies from FI to FI. So, I'm only going to speak for Chase and I really can't speak for my competitors. Your statement that things like an

address change, which is an early indicator of fraud and as the FTC defines it, identify theft, even in transaction fraud, is something that we look at as a high-risk transaction. So, something as simple as the last four of our Social would not authenticate you sufficiently to do that transaction.

We've actually done a full exercise of looking how -- it's actually part of my day-to-day job, when I'm not speaking at conferences. What we did was we actually went back and looked at all transactions used to authenticate, regardless of how you're authenticating, but what do you do, what do I do if I want to change or add a phone number, if I want to add a seasonal address? All those things that now we're talking about red flags, but fraud practitioners like myself have been doing as our daily job for years, we look at that and we determine, based on our evaluation of those risks, whether or not the last four digits of the Social or the full Social are enough.

I can tell you that there's very few, if any, transactions that we offer out under just that authentication measure, but that's not true for every place. And it goes beyond call centers, it goes into the websites and how you authenticate through a website and how you enroll in the services. So, as part of a rolled

out through FFIEC about a year and a half, two years ago, you know, on strengthening authentication, we took that to the next step and took it beyond just online, we took it across the bank.

So, I just wanted to kind of touch upon that because I can say, without a shadow of doubt, if you call in and say my last four digits of the Social, there's not a whole lot of information you can collect from that.

MR. LAMB: And just to supplement that, there was a reference this morning to the secret sauce that goes on in the background, and there really is a great deal of authentication that consumers don't realize is occurring in their interactions, and that's appropriate. Some of our customers are very large online or telephonic retailers who sell computers and the card's not present, somebody might be either online or in a phone situation, and they're using our data to check is the delivery address the address associated with that individual and that name and how long has it been their address.

And when things start to synch up, the fraud factors come down. There is authentication going on, and it's not just have a credit card number. You have to realize that people base their rule sets on their experience as they continue to fight fraud.

DR. ANTON: If I could just add, an

authenticator, to be valuable and rigorous, needs to be a secret. And when the follow-up questions are, can you please provide your current address and your current phone number, these items are published in the phone book, they are not secrets. And, so, I think we're missing the point here. An authenticator needs to be a secret.

Your PIN number when you go to the ATM machine, maybe your spouse knows it, but I doubt you have it published anywhere, and I think we're all very concerned about our financial information, and you never hear about identity theft because somebody got a bunch of PIN numbers, which are only four digits long, but it's secret. And that's the point I keep coming back to because I think we're missing the point and it's very critical.

MR. LAMB: But, Annie, I was talking about the delivery address for the goods, but I agree with what you say as a pure authenticator.

MS. COHEN: This question is for Bob Ryan. I don't know if you can hear me.

MR. RYAN: I can hear you.

MS. COHEN: You mentioned in your opening statement that TransUnion operates globally and I'm wondering if you could elaborate on what the efficiency

or accuracy of your credit files are in other countries that don't have an SSN equivalent and countries that have a national identifier that you had mentioned, I think Singapore and Hong Kong as well.

MR. RYAN: Yes, thank you. I tried to develop that in preparation, in fact, for this when I received the invitation to speak here, and it was tough to get at that figure other than in very stark terms. So, in other words, in South Africa, where there is a very robust, biometric-based national identity number with all the back-up, it's required. They can't accept information, they can't accept public record information into the reporting system without that number. Similarly in Hong Kong.

And when I asked about the impact of redeveloping the system or what that would mean if the use of the national identifier was not just withdrawn but even restricted, it was very difficult for them to even calculate that other than it would be a profound effect on accuracy and completeness. On the other hand -- so, I'm sorry, but it's a big impact when it's baked into the existing system.

In India, the Republic of India where we are also not quite as far along -- we've been in South Africa for a long time, 15 to 20 years. In India, in contrast,

where we have just begun as a junior partner to the banking system, to the federal bank, developing the credit reporting system, India does not have a national identification system or anything like a Social Security number. They have a voting ID, they have a tax ID, but those are only intermittently used by various folks in the population, you know, they're not as pervasive at all.

And they know a lot about this issue and the benefit that would gain to the accuracy and completeness of the credit reporting system in India if they had that kind of a universal, issued by the government, non-changing kind of national identifier. And, again, there, they predict -- I don't even want to throw out the number, but it would be a very significant, you know, plus 20 or 30 percent -- okay, there, I threw it out -- increase in the accuracy and completeness of the system, if they had that kind of a...

MS. ABEND: Can we take that question and just change it a little bit and say, you know, for maybe to Stan, you can comment to this on the phone or, Robbie, talk about what kind of impacts to the customer, in terms of efficiencies or what have you, you think a change in terms of not being able to do the external linkages the way that we currently have it, what kind of impact that

would be to the customers so that that end customer feel might become a little bit more apparent.

MR. SZWALBENEST: So, what you're suggesting is I wouldn't be able to validate credit quality, I wouldn't be able to comply with AML, I wouldn't be able to comply with several laws on the books because if someone presents themselves to be who they say they are, that's all I would have.

The Singapore example is excellent in that there is a strong national identification card process there. But what we also don't have is our population is several times larger than Singapore's, and also, there's the feeling in the United States about how much information we provide the government and how much we want them to credential us. If I was walking down the street in Hong Kong or Singapore and a police officer with no prior causes, show me your ID card, I have to show him my card, and if I don't, I'm going to jail.

So, it's a different environment they're operating under. I'm not saying it's better or worse, it's different. And if we had those credentials here, well, I would simply put it in the card reader in my branch and I'd be able to open the account because it's a biometric and it's multi-factor. So, it's a different environment.

If I sat back and said how could we operate without going to external sources, I really don't know. You know, if you look at the economy today, we've used external sources to validate credit quality and identities and we're sort of in a pickle right now with low doc, no doc loans.

So, I could say things could be a lot worse. We need an identifier to go out just to look at records.

MS. MEYER: Similar to that, I mean, I think our customers expect us to get accurate information, particularly as I was saying before with medical information. They expect us to do it quickly and accurately like when they're trying to get information across a holding company, they call in, they've forgotten their policy number or their account number, they want it to be accurate. I also think that they're concerned about fraud and identity theft.

And I think, you know, my understanding is is that the universal best link to these commercial databases to be sure that we can do our Patriot Act, know your customer, do our criminal checks, not hire people who are convicted of felonies, the best way, the quickest way, the most accurate way into the current system, given the way it's set up right now, is to use these numbers.

So, it's my members' impression that the best

way to prevent against fraud, and we think our customers want us to do that, is to use these numbers.

MR. SZWALBENEST: Well, again, the use of these numbers, it's one element. If we can create some fancy algorithm that converts the number, hide the keys, and that becomes the new number. But as soon as that happens, because I study the criminal element as a profession, they'll social engineer it out of our customers. It's just the way it is. They get paid to do what they do and we get paid to do what we do. They just make more than us sometimes.

MS. ABEND: Dr. Anton?

DR. ANTON: So, I think many of us have heard that moat data breaches and security breaches occur because of the insider attack. We've recently been looking at the cases that have been -- the indictments that have been handed down for criminal HIPAA violations and all of that data was accessed by someone who had access to the information and worked in a doctor's office and then sold the information to someone else.

So, this is why I'm advocating that we use different identifiers within companies, within medical practices, within financial institutions, within the company, the people that have access to those records and only use the Social Security number for external data

linking and have those Social Security numbers in a separate database that's encrypted and is only accessible for the purpose of data transfer.

MR. TOWNSEND: If I may, from an investigative standpoint, we're an old, tried and reliable profession. When we access data, perhaps it should be embedded into the inquiry as to the date, time and the person that made the inquiry. The databases I use, that's exactly what they do. Similar to the PIN number. And that can go across an entire range of needs to satisfy the identity theft requirement.

MS. ABEND: Next question?

MR. SABBETH: Hi, my name is Larry Sabbeth and this is directed toward Mr. Lamb. Most of the remedies suggested on the Hill envision restricting exchanges of Social Security numbers generally with a long list of exceptions starting with law enforcement and national security. Given restrictions such as redacting the Social and other restrictions, will those exceptions really be of much value or will the actual database that even law enforcement is accessing and the national security folks are accessing be diminished by some substantial amount?

MR. LAMB: Well, our concern is under some of the pending proposals to restrict the transfer of Social

Security numbers, we, for example, would not be able to receive accurate Social Security numbers, you know, for the entire array of services we provide to law enforcement, to background screening, to credit and for others. Certainly, partial Social Security numbers are not useful.

There have been exceptions proposed in some statutes. You can use it for law enforcement. But if we have it, it seems ridiculous that we can use it and have accurate linking for one purpose but then we have to say, unfortunately, we can't use it to accurately link over here to help corporate fraud investigations, for example. And then if you add an exception for that, what about finding the pension beneficiary? Once you start to go down the exception list, you really need to be sure you don't accidentally carve out some really beneficial uses.

The entire array of Gramm-Leach-Bliley Act purposes are really what the -- the array of purposes that Social Securities need to be used for.

MR. RYAN: I think another important point I would add to that is that from the standpoint of the three major national credit reporting agencies, which receive, as we said, huge amounts of data from financial institutions containing Social Security numbers, if such an act were passed that created an exception for law

enforcement or national security or whatever, that still -- it would not answer the question whether we would still be able to receive it for the overriding purpose of credit since that would not -- if that were not an exception. And, so, I think that's part of what Michael was getting to. That there would be an interruption in the flow that was not intended.

MS. ABEND: I think we have time for one more question, so the gentleman in the back of the room.

MR. McCARTNEY: Jim McCartney with Bearing Point, representing the Department of Defense. First off, it's kind of a circular argument. The numbers are useful because we use it for so many things, so you can't really go away from it. But my question is: If you had to go away from it, if we went Draconian and said you're not allowed to use it, what would you do? I understand there's lots of consequences, but what would your actions be in terms of trying to contain or continue your business model if you were no longer allowed to use it?

MS. ABEND: I'll start by saying first and foremost, you'll probably have to pass some laws just from the Treasury standpoint because we require it but I'll let the panelists answer.

DR. ANTON: From a technical perspective, there is one study that showed, that was published in the

Journal of Public Health, I believe, that shows they were just as accurately able to identify people using first initial, last name and date of birth or first initial, last name and place of birth in the Social Security death index as they were with the Social Security number.

Now, it's a limited number study. But that shows that there are other ways. But until there's a law that requires that, I don't see it happening.

MR. RYAN: From the credit reporting standpoint, the FTC's report on this, very excellent document that's part of the handout, cited the impact at 15 to 20 percent, 15 to 20 percent drop in the accuracy and completeness of the credit reporting data, and that's what would happen if overnight we were deprived of it and then translate that, what that means over the -- am I not answering? I don't get --

(Participant not at microphone.)

MR. McCARTNEY: (Inaudible) if you didn’t have access. I understand the consequences. (Inaudible) what would you see your businesses doing to try and take an action?

MR. RYAN: I'm answering your question. In the near term, we wouldn't be able to do a darned thing. We would continue operating without Social and there would be this dampening effect which is going to hurt marginal

populations. You think we have a problem now with the bank and mortgage crisis, you know, just take a 20 percent reduction in the accuracy and completeness of the credit reporting system and spin that out a year and then see where we are.

MR. LAMB: Valerie, if I could also just respond to the earlier study, the University of Michigan study on the death index. I was surprised to hear the claim that the linking was just as accurate without Social Security numbers. So, I looked at their study. And among the dead, I think they did reach that conclusion. But among the living who changed names and who moved and I quote from the study, "including Social Security number as a matching criterion significantly decreased the number of false positive matches."

It is a very important link. I don't think we can argue that linking is equally accurate without a Social Security number.

MS. ABEND: All right, we are out of time. I want to thank all of the panelists. I think we had a very interesting discussion. And I hope you have an excellent rest of the workshop. Thank you.

(Applause.)

PANEL 4: SSN USE FOR AUTHENTICATION AND FRAUD PREVENTION

MS. LEFKOVITZ: Well, after the taste of the last discussion, I think this panel should prove to be an exciting end to the afternoon. But, first, let me thank all the panelists for being willing to share their expertise today and let me go ahead and introduce them.

So, first, we have Beth Givens who is the Director of Privacy Rights Clearinghouse. We have Trey French, a Vice President at Bank of America; Emily Mossburg, Senior Manager, Security and Privacy Services at Deloitte & Touche; Jonathan Cantor, Executive Director for the Office of Public Disclosure at the Social Security Administration; Jennifer Barrett, Global Privacy Officer at Acxiom Corporation; and Tom Oscherwitz, Vice President of Government Affairs and Chief Privacy Officer at ID Analytics.

So, clearly, if we could always identify people correctly we wouldn't have any identity theft, and while this may be stating the obvious, in essence, authentication, the process by which individuals are accurately identified is the topic we're exploring in this panel. In particular, these panelists will be discussing the ways in which SSNs are currently used in this process. Some of the questions we'll be trying to answer include in what ways is SSN use inappropriate and

can it lead to greater risk of identity theft and in what ways can SSN use improve authentication and prevent identity theft.

Finally, I hope we'll uncover whether there are alternatives to using the SSN for authentication and how viable these alternatives may be.

So, let me first turn to you, Beth, and what issues do you see in the use of the SSN for authentication?

MS. GIVENS: Well, to deal with that rather large question, I would like to describe the work that we do at the Privacy Rights Clearinghouse. So, let me start off just saying that the Privacy Rights Clearinghouse is a nonprofit consumer advocacy organization based in San Diego, established 15 years ago in 1992. And a real quick description of what we do is that we're kind of a "Dear Abbey" of privacy. We invite consumers' questions and complaints and we do the best that we can to troubleshoot them.

To answer those many questions, we've got over 50, five-zero, guides on our website covering a wide variety of informational privacy topics, and the top issues that come to our attention every day are identity theft, credit reporting, employment background checks, medical records, and Social Security numbers. So, if you

think about it, each of these topics, actually Social Security numbers are a major component within each of these subject areas like identity theft.

And I'm not going to get into identity theft, but there are various kinds, there's financial, medical and criminal identity theft. And for each of those, illegitimate access to and use of the SSN is a major component.

Based on what we've learned from consumers over the years, it's no understatement that the majority of people who contact us range from the very uncomfortable to the downright angry about the many demands for their Social Security numbers from the private sector.

Now, our panel is on authentication and how the Social Security number is used to verify or confirm the identity of individuals, and I have to say this, there's going to be some duplication of content in what I'm saying to some of the last panel's participants and we didn't get our heads together ahead of time. So, I just want you to know that this is all independent and maybe it points out the importance of some of these points that more than one panelist is actually talking about them.

We've heard about the identifier issues in that panel. In that situation, the Social Security number is being used to answer the question who are you. But when

the Social Security number is being used for authentication, it's basically being used as a challenge, prove who you are, and herein I think lies a great deal of the discomfort and anger that we hear from individuals across the country who contact us.

The Social Security number has evolved over these past 70-plus years to be both an identifier and an authenticator, and as Bruce Schneyer or Schnear (phonetic), if you were here I'd ask him to pronounce how to pronounce his name --

UNIDENTIFIED FEMALE: Schneyer.

MS. GIVENS: Schneyer. In his excellent book, Beyond Fear, he says, that conflating these uses as both an identifier and authenticator and failing to distinguish between one and the other can lead to a lot of serious problems. And I think we're seeing those serious problems in financial identity theft, criminal identity theft and medical identity theft.

The FTC staff report, which is excellent -- and thank you all of those of you who worked on it, it was very useful -- explains that authentication is dependent on individuals presenting some sort of factor to prove their identity before, for example, gaining access to a financial account or a computer network or an online resource. And by the definition of authentication, those

factors should be something not generally accessible. Something a person knows -- I'm repeating Dr. Anton here, something a person knows like a password, something a person has like a physical device or a token or something a person is like their fingerprint or the pattern of veins in their eyes, biometrics in other words. This trio of factors, what you know, what you have, what you are is a standard scheme in the field of authentication.

Now, unlike identifiers, authenticators are supposed to be secret or entirely unique to that one person and not widely known, actually not known at all to others and, of course, Social Security numbers fall into that category of something that not only you know, but an awful lot of other people and entities know. It's not all that difficult to obtain it if you really are bent on it.

A few years ago, I participated in a hearing that Senator Dianne Feinstein and Senator Jon Kyl had. This was before information brokers started working with each other and making their databases less accessible. But I went online and for $25 purchased my own Social Security number. Anyway, it's not all that difficult to get people's SSNs. Even today, after the information broker industry has done many things to try to keep the Social Security number just in the hands of those with a

legitimate need to know.

The problem with a Social Security number -- okay, I'll be able to finish in one minute -- the problem is it's widely known and it's not all that difficult to obtain. In researching for this presentation, I learned a fair amount about multi-factor authentication and I think that's really where things need to go. It's an understatement, really, that the Social Security number is not appropriate at all as a sole authenticator, and I think that's what's happening with identity theft. It's unfortunately, I think, weighted -- I'll borrow the term from the last panel -- I think it's weighted and it is being used as a sole authenticator, at least in terms of credit-issuing.

But it does have its uses as an initial identity verification tool to facilitate other forms of identification -- or, I'm sorry, to facilitate some other forms of authentication like developing knowledge-based questions.

I just wanted to read -- well, I think I'm going to skip over that, but there's an excellent report that I -- the Federal Financial Institution's Examination Council and I was going to read about the importance of multi-factor authentication. They mention that a lot in their report and they don't mention, by the way, the

Social Security number at all in the entirety of that report.

This is not the first time we've addressed Social Security numbers. Back in 1977, the Privacy Protection Study Commission devoted a whole chapter on the Social Security number issue and all of its multiple uses. So, we're still facing this 30 years hence. I want to commend both the President's Task Force on Identity Theft and the FTC for bringing up the Social Security number as a significant issue and, specifically, the authentication issue. I, myself, am one of those who believe that the Social Security number should not be used for authentication. And thank you very much.

MS. LEFKOVITZ: Thank you, Beth.

Trey, what role does the SSN play in your bank's account opening process and how you authenticate individuals?

MR. FRENCH: Sure, Naomi. First off, I'd like to thank the FTC, Naomi and Kristin also for inviting Bank of America to this panel.

Identity theft or preventing identity theft is a key focus for Bank of America. It's a key focus for having a competitive advantage against the other financial institutions out there. When we get right down to it, banks are in the business of making money, hitting

the quarterly interest earnings report. Any fraud loss to the bottom line hurts us and, in turn, if our customers leave us because they don't feel like we're protecting their information that hurts our bottom line. So, at the end of the day, when you look at the basics of this, ID theft prevention is key to banks moving forward and earning and meeting their corporate goals. So, hand in hand, this is important to us.

Three key points, and I'll get into, Naomi, that question. ID theft poses a huge risk to financial institutions. Banks take active steps in preventing ID theft. And it's been going on or we've been trying to prevent identity theft long before Gramm-Leach-Bliley was passed. Credit has been being issued and regulated by Regulation Z, the Truth in Lending Act, since, I want to say, 1969. And when you look back to the fraud provisions within that, there's points there where it talks about how consumers can remedy or how they need to remedy ID theft situations.

What I first want to talk about is what our customers are telling us in terms of authentication. And there's three points that Robbie Meyer on the last panel talked about as far as authentication goes and what she believes and what she believes the public is saying.

For Bank of America customers, here's what

they've been telling us. Seventy-four percent of our customers have said security of personal and financial information is the most important feature of the authentication process. Ease of use and transaction speed is secondary to that. So, they're telling us they want us to keep their information secure. In addition, they're also telling us that consistency is not that important.

So, if I had a wealth management account and I'm a millionaire and I move money all the time, that requires one level of security as opposed to I'm a credit card customer, that may pose a different level of security because it presents a different level of risk for the customer, in their mind, as well as the business. So, looking at that, what we've noticed is we have to take a varied approach, one approach to our online customers, one approach to our wealth management customers.

Moving on to kind of how we go about the process of authenticating our clients from an open end credit perspective, new clients, to existing customers, you have to go back to Section 326 of the Patriot Act that I think it was Valerie who was on the last panel spoke of, and not to dig into the same stuff we've already talked about, but identification or collection of

information is a key factor. What do we have to get? What are we required to get by the federal government?

Well, we're asked to get the name, the address, physical address, Social Security number or identification number and date of birth. When we look at the identification number, what is that? Well, as Valerie, I think, mentioned before, the identification number for U.S. persons is their tax identification number. In essence, that's the first level of authentication.

We also look at a lot of other things that Acxiom and other folks up here, LexisNexis, can talk about in further. It's not just matching up that data, the data the customer has given us to the data that is on the credit bureau. It's also looking at how often this person has applied for credit. Does this perhaps tell us that it may not be the person applying? Maybe you see five inquiries over the last week. Well, that might be an indication of ID theft. Was there a recent address change? That may be an indication of ID theft. There are a lot of things behind the scenes that I think the folks up here from the credit bureaus spoke about earlier that occur when we're trying to identify customers. It's not just verifying the information, the four pieces of information through the customer identification

procedures.

Moving into existing customers, we have various voice response unit or VRU strategies and it's not just keying in the last four digits of the Social Security number or keying in the full Social Security number that drives a customer in and we kind of give up the whole thing. That's not the case. If a customer is trying to do a balance transfer, a Social Security number might be one of the pieces we ask for. But once we get to the representative, it may also be something related to another account that the customer has with us. What's your balance on your car loan?

I'd say about 25 percent of our customers have multiple relationships with us. Meaning that at a representative level, when somebody's looking at the account, they can also see how that other relationship interacts and they can also use those pieces of information to help authenticate that client.

Through our online system we have something called secure key. Under secure key, that allows us to give a password to the customer. So, you have your front end using your user name and password. Then once you get into that system we ask you for another password that is then authenticated and that's how you get into our online banking system.

There's a whole bunch of other stuff that we want to talk about, there's some survey stuff that I want to share with you as well. The bottom line is all financial institutions have a stake in protecting consumer information. And at the end of the day, consumers will go to the banks that do the best job at securing information.

MR. LEFKOVITZ: Thank you, Trey.

Emily, how have you seen the SSN being used by financial institutions for authentication for existing account access and including online and on the phone and has there been a change since the FFIEC guidance?

MS. MOSSBURG: Thank you, Naomi. Before I start, I want to thank the FTC and Naomi and Kristin for getting this conversation started because I think that these forums and bringing together all these people is really what it's going to take to address this issue, because the Social Security number is so embedded in so many of our systems and used in so many different ways today that we really need to work together across industries, across organizations, and with the government to figure out how we can protect the Social Security number and how we can minimize identity theft.

In terms of authentication using a Social Security number really as you said, Naomi, there are

three ways that people authenticate or three ways that you need to authenticate people. In person, online and via the telephone.

In person, people are obviously there, they have their IDs, those are usually used for authenticating them and they have signing cards.

Online, what is usually used is a user name and a password. The Social Security number is usually not used to log into an online system. However, there is another aspect to that and that is setting up an online account and in the process of setting up an online account the Social Security number may be one of many pieces of identification that is used. So, there is some degree of authentication there, but on a day-to-day basis it's usually a user name and password that's used. And in some cases, going back to the FFIEC, some financial institutions have moved to a multi-factor authentication approach. So, using user name and password as well as another piece, as Beth said, moving toward multi-factor authentication is an option. And I'm going to talk a little bit more about that as I go.

From a telephone perspective, Social Security number is often used by financial institutions to authenticate as one component of the authentication process. And the process that usually takes place is a

multi-step authentication. I won't call it multi-factor because it's usually a series of questions, so I would refer to it as multi-step authentication, and one of the questions that may be asked is Social Security number. But, again, there's often a lot of other questions that are asked, mother's maiden name, address, they may ask about a past transaction, et cetera.

One of the things that's also happening in terms of telephone authentication, though, is movement to a pass phrase and implementation of a pass phrase so that it's similar to having a PIN, having a password, et cetera. You have a particular password that you use when you call to make a transaction. This, of course, leads to further complications simply because there's process changes that are required for a financial institution to implement something like that and there's additional complications when people forget their pass phrases.

I don't know how many of you forget yours, but I know that several times I've set them up and then I forget them when I call because I very rarely call that bank. And, so, then you've got the issue of, okay, how do we go about resetting those, how do we authenticate the user when they forget their pass phrase, as well as there's some level of expense and resource that needs to go into making sure that you're validating a person and

putting in place a process to authenticate them if they've forgotten their pass phrase.

In terms of the FFIEC guidance and changes we've seen based on that, I guess what I would say is there's a number of regulations and industry standards that are really pushing change in terms of authentication. But I would say that really it's not so much about the use of Social Security numbers, it's really more about protection of the data. How do we protect personal information, what safeguards do we put in place, and if there is a breach, what do we need to do? Because I would say that a lot of what's pushing organizations today revolves around the state breach laws that are out there and the notification process that's required if data is breached.

And I'm just going to close on one thought following up on what Beth said around multi-factor authentication. It's definitely a great option. I think it is a very complex option and potentially a very expensive option, so I think that it's something that we really need to put a lot of thought into in terms of how do we implement multi-factor authentication in a way that is actually operationalizable and is workable for organizations, and it also opens up the large question around federated identity and moving to a federated

identity. So, with that, I'll close.

MS. LEFKOVITZ: Thank you.

Jonathan, what tools does SSA make available to companies to assist them in fraud detection and authentication? There seems to be a lot of confusion. Can any business match an SSN to a name for authentication purposes with the SSA, and if not, why not?

MR. CANTOR: Okay, first of all, I'd like to join my colleagues in thanking the Federal Trade Commission and you, Naomi, and Kristin for setting this up. Thank you for inviting us to participate.

I guess I don't really need to tell you much about the Social Security Administration. I think most of you are familiar with us. But we're obviously a major federal agency, we assign the numbers and, in addition, we pay some benefits that you might have heard of along the way.

I definitely wanted to talk to you a little bit about some of these points and it's interesting that you actually ended on the point of federated identity, which is a point I'd like to talk a little bit more about later in the panel. In terms of fraud detection, one of the most important things to remember about the Social Security number is sort of how it works. Social Security

numbers were created primarily for Social Security's internal use and that was designed to help us administer a program that would touch the lives of people all across the country. As we all know, they're widely used across all levels in the government and in the private sector, and they went from our narrow purpose to sort of becoming, as several of the panelists before me have said, a de facto national identifier.

Really the driver behind that was probably the lack of any other alternative and the lack of regulation that said you couldn't do that. We all know there is no blanket federal law that prevents non-governmental entities from using the numbers. And collection and use limits, to the extent that they exist out there, are really targeted at the government.

In addition, as we've heard, there are many laws that require the use of the number at the state and federal level. Nowhere in any of these laws is there a requirement to use them for authentication. They're primarily used as one of many identifiers, as several previous panelists have pointed out. And, indeed, as several folks have pointed out, the use of such a publicly available identifier, similar perhaps only to the name in terms of just how publicly used and available it is, is probably not such a logical choice because

you're really trying to focus in on an identifier that's not well-known when you're using authenticators. And, actually, as Professor Anton pointed out in the last panel, it really is just an excellent identifier and not much more than that.

So, looking in terms of fraud detection, one of the most tools is to think about how the number's assigned, and as you always see it, it's three digits, dash, two digits, four digits, and each of those parts of the number have a different name. The first three digits are called the area number and the second two are called the group number and the last four are called the serial number. The area numbers are assigned geographically by states. The lowest numbers are assigned to the New England area, and then to the Mid-Atlantic, the Southeast, the industrial Midwest, the rest of the Midwest, the Mountain West, the West Coast, Alaska and Hawaii, and they just kind of go through that numerical progression.

The group numbers that are those second two digits, those are assigned in sort of a strange pattern, 01, 03, 05, 07, 09, and then we move to the even numbers, 10 through 98, and then we go to 02, 04, 06, 08 and then odd numbers, 11 to 99. And in each of those group numbers, the serials run sequentially from 0001 to 9999,

and then we go to the next group number and do the same thing, we never use all zeros. And there's no real logic to that, it's just sequential. The reason I pointed that out for fraud detection purposes was a number can be isolated pretty quickly by knowing generally from what area of the country a person is from and about when that person was born.

So, on top of that, we have sort of a strange interface with the Federal Freedom of Information Act because enumeration is a service that Social Security provides to members of the public and, so, a lot of information about that process and how it works is actually available to the public and is on SSA's website and is well-known. And, so, we actually explain how and when these series are used and things like that and they're up on our website. Not the actual numbers, but a lot of information about completed groups.

And then, of course, we also work directly and closely with lots of employers, and they have asked for that information over time. And as kind of another strange interface with the Freedom of Information Act -- and this is going to segue me into the death master file as many people have heard it called -- we actually release a large file containing over 65 million records of individuals who have died and their Social Security

numbers. And the demand for this file is so high for anti-fraud purposes and genealogy purposes that it's actually available for sale through the Department of Commerce's National Technology Information Service, and most of banks and credit bureaus subscribe to it. It's a useful way to actually kind of strike a Social Security number off of your list because we never reuse a Social Security number.

Some folks earlier in the day had talked about that there is an obvious end to the number of Social Security numbers, and one of those reasons is because we will not reuse them.

So, just in terms of thinking how the number itself works and that death master file, the other pieces in terms of working with employers, while we verify SSNs for purpose of employment because that's actually kind of a core essential purpose for why the number was created, we need that information to be able to report wages to your earnings history.

We are not able to verify or disclose SSNs to a private industry due to the limitations under the Federal Privacy Act and that, obviously, is just that simple compatible notion, it's not why we have the information and why we collected it. So, we're sort of limited there. But Social Security, due to demand, is creating a

fee-based service for entities that are willing to collect individuals' consent and with the individual's consent the service is called the consent-based Social Security number verification service. It is not yet live and it's still very much in its early deployment phases.

There will be more information coming, but if you would like to go to Social Security's website and find out a little bit more about that, it's in our business services online. There's a mail serve to which you can subscribe to find out more. But that particular tool will probably be the largest tool that Social Security can deploy in terms of working with people on Social Security numbers.

MS. LEFKOVITZ: Thank you.

Jennifer, what types of tools do data brokers offer to assist businesses in authentication and what role does the SSN play in making those tools available?

MS. BARRETT: Thank you, Naomi. I've got some slides, too.

MS. LEFKOVITZ: Come on up.

MS. BARRETT: Thank you, Naomi, and thank you to the FTC for inviting us. If there was an easy answer to this question, we would have found it by now and I think based on the debate we had this morning and this afternoon, it's obvious that there aren't a lot of easy

answers.

I would like to start off by really kind of talking about -- we've alluded to this, but I have a chart that kind of talks about this, what I call the spectrum of authentication. And it's driven by a lot of different factors. We see very low need for it in certain activities and then we see a very high need for it in other activities. But there are a couple of things that come into play here in identifying where you fall in the spectrum and where we see the use of SSN.

How much is at risk? Is it pretty low if I'm renting a video and I'm out nothing but the dollar it cost me to create it or if I'm applying for a loan or even applying for employment?

We talked earlier about the consumer perspective on this. How much time and money is it worth both to the consumer as well as to the business to go through an authentication process? And, obviously, any steps you take are not free, so we have to take that into consideration. And then does it make sense to the consumer? Consumers are starting to push back, as we've talked about, about not wanting to give their SSN. Beth gave an example this morning about using a driver's license in lieu of an SSN. So, all of these have to be taken into account.

But what we have seen over the last decade is the use of SSN in this process has migrated further and further up the scale, and I think that's a recognition that it is an important, but a potentially dangerous, variable if it falls into the wrong hands and so one that we all need to take special precautions around.

Now, where does Acxiom and information companies like us play in this process? This chart kind of depicts the whole process from starting out with I enroll in something or I sign up or I apply for something, and then that creates a credential or an ID from that particular entity, maybe with a PIN, and then I use that, you know, in various transactions. Acxiom plays a role in two parts here. We play a role in validating the information at the application or enrollment stage, and I'll talk about both of those in a little bit more detail, and then while we're not going to talk about it on this panel, but in the interest of disclosure, we also provide tools and services to investigate suspected transactions that are known fraudulent situations on the back end. So, we play in both of those arenas.

We are seeing more and more sophistication in the enrollment phase. As you can see from this chart, SSN plays a much more important role in the enrollment or

application stage than we are seeing in using the credential. People are moving further and further away from requiring it when you use the credential. Other than, as was discussed in the panel earlier, when I have lost my credential or have forgotten my PIN and I kind of need to go through a pseudo re-enrollment application.

We actually offer two products in the validation of the enrollment or application information. One that is geared toward kind of general business use and one that is specifically geared towards employment. The general account authentication offering that we have allows our client to validate the information that you've been presented by a consumer.

I've given you three different screen shots here. Because what we actually do is we actually score the data when it comes from the consumer and we provide the client with the score with our confidence factor of how much we believe the information correlates to each other. So, you can see a very low score of 74 here. That indicates we have a lot of data that doesn't match up. Whereas a very high score of 496 says basically it's all matched up.

In this process, our client can either log on to the system and enter it into an application that we provide them or we can provide a direct feed into their

own application process and have this score interpreted by their system and then a determination made about what they do with it.

Typically, there are three kinds of actions that take place. Based on the score, they either decide to move forward with the rest of the application process, because we are not certainly saying that they are eligible for this loan, we are simply saying that the credentials that they presented do all match up. It may be such a horrible score that they want to deny the application process and ask the consumer to start over. But probably more likely they will ask to go to kind of a second phase of this, which is where we present additional questions that we discussed earlier in a couple of the other panels, the concept of out-of-wallet questions, things the consumer would know or maybe have with them but not readily known or easy to steal. Those would allow a consumer to maybe get past not having the right information or having some of it in error.

Obviously, we get things like transposition errors, particularly if I'm entering it online myself or if someone is keying it in for me, and those are things that have to be taken into consideration. Not everybody that doesn't pass with a 496 is a criminal.

It's important to note that in this application

no new data goes back. We're not actually providing the client with any information they didn't already have. We are simply trying to help them sort through what information was given to them.

And, finally, I want to comment that behind the scenes in bringing the databases together that deliver these scores and this information, we use a variety of sources, both public and private, some of which contain SSN. Although we see a growing number of them not having SSN as time goes by. I would correlate the fact that multi-source confirmation in building these truth databases or these knowledge bases, for which we can do knowledge-based authentication, is as important as we have talked about multi-factor identification being important to the authentication process.

I've been asked many times by lots of different people, well, what's the error rate if we took SSN away? Most of us in this industry believe that we've got these systems that validate someone's information to a 98 or 99 percent degree of accuracy. If we take SSN away, we are likely to see that drop to more like 90 to 95. Now, 95 doesn't sound real bad, but if you look at it the opposite way, that is, if it's 1 percent error today, that's a 500 percent increase in problems that we're going to throw into the workplace.

The other part of our authentication services are employment verification, it's the pre-employment verification, verification of the application. One of the things that we do that is a little different from others is we don't amass databases, in a sense, we actually receive an application. This is all governed under the Fair Credit Reporting Act. We send field agents out to verify if you have lived in a certain place, if you say you worked for a previous employer, if you have a certain education, we contact the university or the college, et cetera, and we pull together a composite report of this.

One of the things that we also do is a criminal records background screen. This has become more and more required and more and more common in the last few years with the Patriot Act and other requirements, particularly around critical infrastructure. And SSN plays a key role in this, in all of these verifications. Obviously, missing a conviction as a sex offender if you're applying for work in a day-care center is pretty serious. But so is, conversely, accusing someone of being on one of those registries when they're actually not. So, we have both sides of that equation that we need to worry about.

This report is sent back to the employer and the employer is obligated to tell the individual, first

of all, they signed off to get permission for this to happen in the first place, to give a copy of the report back to the individual so that if they want to challenge it or question anything, they have the certain right and there are processes defined for that purpose.

I wanted to conclude by just making a couple comments about protecting SSNs. I think it's extremely important that the security around any kind of sensitive information, and we certainly consider SSN as sensitive data, be very high. We go to extra lengths to credential the clients that we offer these services to. We make sure they're legitimate and appropriate, have appropriate use for the data. Anyone using the system online, we enroll in an IP address and their enrollment and their logon is tied to that IP address so they can't move around, it can't be done with laptops, they can't go to an Internet café and do these kinds of things.

We also do site inspections of anyone involved with any of these services that use SSNs and we do some periodic re-credentialing.

The other part of this is logging and monitoring transactions. Sometimes you can spot a guy before they're caught by actually tracking kind of what's happening and saying, wait a minute, this is really aberrant behavior, and also, following up then with our

client or, in some cases, law enforcement if necessary.

I'd just like to conclude by saying that SSN plays a key role in high-risk authentication, and I don't know of an equivalent substitute. However, I think if we begin to continue the process of phasing it out in lower risk transactions where we really don't need it and we move to more multi-factor authentication and reducing its use more and more just to the application or the enrollment phase that we can begin to continue the improvement we've seen in spotting and detecting these criminals earlier in the process or even before they get into the act. Thank you.

MS. LEFKOVITZ: Thank you, Jennifer.

Tom, can you tell us about how quantitative fraud prediction models work and how the SSN comes into play?

MR. OSCHERWITZ: The short answer is I hope so.

MS. LEFKOVITZ: I have confidence.

MR. OSCHERWITZ: I also have slides. So, by way of brief introduction, ID Analytics provides identity risk matching services for many of the nation's leading wireless, financial, and retail organizations. And what I'm going to try to do here, and we've had some discussion throughout the conference, is this sort of "Wizard of Oz," what goes on behind the curtains. So,

I'm going to try to, in my very brief period of time, talk about how in some advanced quantitative identity management models SSNs are actually used.

So, one thing I should say about how ID Analytics technology works, and different technologies use different approaches, is we look at the relationship among identity elements. And I'll show you going forward, the bottom line here is that, yes, SSN is one of the factors that we do use in evaluating identities, but it's not necessarily the most determinative factor.

The other thing I would point out here is we live in the era of the Internet where a lot of basic identity information is quite readily available. So, operate under the assumption that the SSN is available to fraudsters so they are going to get access to it, and what we focus on is how fraudsters use that information because one thing fraudsters cannot do is hide their tracks. Their behaviors are in the sand and you can see what happens.

And, so, for folks here it can be a little hard from this angle, but what we have here are two basic identity patterns, a good and a bad pattern. For folks who can't see, there's a figure of a person, the birthday cake is their date of birth, the key is their SSN. What we see at the top is a plausible identity pattern, where

you have two individuals with two names living at one address with two Social Security numbers and two phones. And that's quite possible, you know, a lot of folks live as a couple and they have two phones and they share the same address.

Now, in the second pattern we have here, we have two people sharing the same Social Security number. Not necessarily a good thing from an identity confidence level. So, that's a very, very basic description of how, on a space relationship, identities look more troubling on the second chart than the first.

Now, it's not only space but time that you can look at how identities behave. So, again, we have the first example here, we have two identities sharing the same address. Here you have two different phones and there's an application made for a credit card, for example, and then, all of a sudden, there's a second application. Nothing that's suspicious here.

But what happens if there's a third application and that third application is known to be a fraud? Suddenly, the way you think about application number one and application number two changes because now you know that the second application shares a phone number with the third application, so that raises some suspicion. So, you can see when you're looking at behaviors of

identity elements that changes over time and how these identities relate to each other can inform you of the behavior of that identity.

Now, these are very, very simple explanations, so I want to give you some more complex examples. This is sort of the classic law school example where you have 40 different problems and can you issue spot. And what you have here is an individual applying for a credit card. What we have is an ID number, can we look at relationships among identity elements? So, I'm going to start at the top of this page where you see that individual in the middle and there's three Social Security numbers above him or her and there's a date of birth. One example we might have a suspicion about an identity is the date of birth occurred after the date of SSN issuance. That would be an example of fraud.

In the middle of the page, you see a lot of individuals around the house, and that's because those individuals are little triangles which means it's an invalid SSN. What that shows there is that this person is applying from an address where actually it turns out in our network there are a lot of other individuals at that address and some of those have fake SSNs or fraudulent SSNs. So, that’s, again, indicative of fraud. So, we're looking at the relationships.

Now, let's get out of SSNs entirely. If you look again at that center individual he's connected to two houses, and what that means in this example is that suddenly an individual is applying for a credit card at two different addresses on the same day. Now, I think that's somewhat unusual. It's certainly possible, but it's unusual for people to say, heck, I need a new credit card and I'm going to get one at this address and then I'm going to go to my summer house and get a credit card there. So, those are, again, anomalies that you can look at identity elements and see how they relate.

One last example would be in the bottom left, we have four people sharing the same cell phone. Now, my experience with cell phones is that prices are going down, right? So, the odds that four people would suddenly be sharing the same cell phone is, again, an indicator of identity risk.

So, what this sort of indicates is that SSNs, yes, they are a variable in evaluating identity, but they're certainly not the only variable. And when we've done our studies of the predictive value of SSN in our fraud models in terms of predicting identity theft, they do provide a lift, a 10 to 20 percent lift. But if you look at other variables like address or phone number, they're, in fact, more predictive of identity fraud than

SSNs. So, one thing to say is it does provide value, but there's actually other identities that are actually -- or elements that are more predictive.

The other thing I'd point out that in the wireless phone industry, we have clients there, 40 percent of the applications of our customers don't have SSNs, but we're still able to build fraud models without it. So, it is possible to build a fraud model without SSNs, but then the question then becomes, what is the cost and what is the value in terms of the costs to society to restrict SSNs? It's going to take a lot of money.

One speaker earlier today said it cost them $8.9 million to get rid of SSNs out of their organization. Then the question is, how much lift are you going to get by removing SSNs from the equation? So, that's one point. So, that's another point I'd like to make here.

For the time being, I think I'll stop there. But I'm happy to talk more when we get to the questions.

MS. LEFKOVITZ: Thank you, that's great information. Coincidentally, in the last week, I actually had to call a couple of my banks about some issues, and one was a large bank and one was a smaller credit union. And I have to say they both asked me for

the last four digits of my Social Security number, my date of birth and my address. So, maybe like semantically they didn't ask me only for my Social Security number, but I can't say I was incredibly reassured by being asked for two other relatively public pieces of information.

So, to what degree are companies, in fact, using the SSN as an authenticator or are they taking other authentication measures that are not apparent?

MR. FRENCH: I'll tackle that question. One of the things that I didn't get a chance to talk to earlier was, ironically enough, Naomi, the point that you're bringing up now, our customers are dissatisfied with the use of Social Security number, date of birth and card number as those common themes of identifiers. So, does it happen? Yeah, you know, I'm not going to say it doesn't happen.

What I'll tell you is that at Bank of America, our policy is when you start getting into, I'd say, a more secure transaction outside of your balance, what your balance is, what your last payment was, when did your payment post type of questions, you get into a secondary level of security. If you're applying for credit, as an example, or an extension on your $5,000 credit line, maybe you want to go up to $10,000, you go

over to a different area. At that point, they won't assume that you are the person, they'll get into questions of, what other card do you have with us? You'll get into questions of, what was your previous address? So you get into some of the questions that Beth, I think, spoke of earlier, the things that aren't as common to the initial relationship. Those uncommon questions that you start to look at.

I'd say you get into that space when applying for credit. You get into that space when you're talking about a balance transfer. You get into that space when you're talking about the level of risk heightening. So, I forgot who, but other people on this panel talked about when you use a Social Security number as far as the risk going up, and I'd say that our questions, depending on the type of activity, we get into more analytical questions to get more information out of you to make sure you are who you say you are.

MS. LEFKOVITZ: Anybody else want to comment?

MS. BARRETT: I'll just make a couple of observations. The interest in doing more authentication beyond SSNs grows every year. And while I think that we're struggling for how many more variables, out-of-wallet is becoming more and more common and more and more prevalent. We are beginning to see a little bit more

interest in biometrics, voiceprints and fingerprints and other things. Obviously, they can't be used in certain spaces or certain distance applications, they don't work as well. But I think we're beginning to explore those.

I mean, the challenge there is making sure that you've got it right when they enrolled because if you get it wrong then everything else is kind of downhill from there.

MR. FRENCH: One additional point. Something that we've noted in surveys and the survey that was done by -- and I'll give you guys the information -- Javelin Strategies and Research 2007 Identity Fraud Survey Report. And three things came to light that impact all financial institutions, and I'll just go over those real quick. This is how customers react when they're victims of ID theft. They avoid online purchases, that's 48 percent of the respondents. Half of the customers say I'm not going to transact online. That's a huge revenue stream for financial institutions. Twenty-eight percent say they spend less money. So, more than a quarter say that they don't use the card as much. And one-fifth, 19 percent, say they switch financial institutions altogether.

So, when you see that information, you start to

realize how important preventing ID theft is to financial institutions to the bottom line. So, again, I can't help but reinforce that point, that it is a key issue for financial institutions.

MS. LEFKOVITZ: Did you want to say something?

There have been a number of surveys, ours included, and the numbers vary somewhat, but give or take, there are about 3 million consumers a year who are falling victim to new account openings. And I guess we just have to question, I mean, we hear that there are these authentication measures, but is this saying that these authentication measures aren't robust enough or, to put it bluntly, is this three million just sort of marginal error in the world of credit opening because there's so many? Can you speak to that?

MS. MOSSBURG: I think part of the issue is the fact that when you're talking about opening new accounts you're talking about passing data from multiple institutions, and instituting authentication mechanisms that span organizations is very complex, again, getting to the point of a federated or a national identity. Because there's only certain things that you can know about a person that each organization can understand.

Right now, the way that our businesses and our financial institutions are set up, we're not sharing user

names and passwords across organizations so there's only certain questions that you can ask and a lot of information is becoming more and more public as more and more information goes online.

MS. BARRETT: I think when you look at it from a criminal perspective, what we see is we see people moving up the authentication spectrum to try to create a false identity. They may start out with utilities where the risk is reasonably low and, so, the authentication may not be that high, but then, as my chart showed, that document they give, that utility bill then can be used to validate that they are who they say they are when they apply for something else. So, there is something of a creeping factor that I think we need to recognize and figure out, either do we need to back up to the very beginning or are there certain documents that are not well scrutinized when they're initially issued and, therefore, they shouldn't be used in subsequent validations.

The other thing that I think is maybe a factor in terms of looking at the number is I don't know that we have a good handle on what's happening with account opening numbers. If they've doubled in the last 10 years and identity theft has held study or gone down, then maybe we actually are having a positive trend that we

don't know about. But I don't know that we know that in terms of how many accounts are being opened and, therefore, what are the percentages of those that actually fall into the fraudulent category.

MS. GIVENS: Referring back to Chris Hoofnagle's presentation on synthetic identity theft, just looking at those numbers and also just looking at what you said there, about three million victims of new account fraud every year, I think it begs the question is any authentication being done at all in the issuing of new credit for there to be so much identity theft, specifically new account fraud each year?

And if the SSN is being used as an authenticator, again, it kind of begs the question, how is it being used as an authenticator? I mean, what's being done? So, I think in terms of -- remember years ago cell phone fraud was a problem. Maybe you can speak to this, Tom -- well, maybe not -- but I think that it's gone down a great deal. But, anyway, I'm of the opinion, and it may be a little bit too pugnacious on my part, but I'm wondering if really any real authentication is being done because of the fact that there are so many new accounts fraudulently generated each year.

MR. OSCHERWITZ: I'd like to add to Beth. A couple thoughts here, I want to sort of go back to first

principles, which is think about the challenge that you have when you're authenticating an individual. A third-party comes to you that you've never encountered before and they present information to you, how do you verify that individual is who they say they are? In small town America where you have a couple hundred people, it's one thing, but when you have hundreds of millions of people living in society it becomes a much more complex issue.

The second observation I would make is that we've had a phase change in our society where there's whole new channels of interactions that individuals have with each other. There used to be correspondence, now people can get access to cards through different services, and a lot of folks like the speed of use, and there's also been changes in the way that people are evaluating identities.

I can certainly speak from our perspective from ID Analytics that the clients that we work with have had significant reduction in fraud loss and it's because they're now using more advanced techniques. And I'm sure that is true for a lot of the other organizations in the technologies that are working that this is making a lot of progress.

So, I guess the question is, is the glass half full or half empty, and I would say that given how

devious criminals are it's sort of like an arms race, one group tries one thing, they come up with a solution, the other side comes up with a solution. I would say that there's been a lot of progress made in the last couple of years to bring down identity fraud. There's obviously a lot more work to do. And I know everybody at the table is committed to that, but I think there's been progress made.

MR. CANTOR: I just want to jump in on one point there, and I agree with everything that you were just saying. I just think it's really interesting you were talking about a lot of progress that institutions have made and I, largely, from the consumer perspective being a consumer myself, have noticed that with the larger institutions I deal with, but in terms of a lot of smaller businesses and smaller financial institutions, I still think there's a great deal of lag there. And I think a lot of institutions and entities lulled themselves into a false sense of security and they do still rely on things like the Social Security number, and it's those difficult new first time transactions where it's like, well, you know, I asked six or seven questions and one of them was the Social Security number, but they all seemed to check out.

There are entities that aren't investing a lot

in doing checks through yours or Jennifer's types of organizations because they don't have the resources or they're making business choices not to do that and they're accepting the risk, and it does kind of set off that arms race because they've now created a bad account on someone else's identity and that definitely does create a lot of problems down the road.

And it's that false sense of security by checking one or two identifiers that are so widely available that still is quite destructive.

MR. OSCHERWITZ: One other quick comment. First of all, I'd like to say I completely agree with Beth about the use of SSN as a sole authenticator. We're in a society now where that simply is not a pragmatic or appropriate security practice because of the wide availability of SSNs.

But the second question is, and I think we're in a forum here where it's worth discussing, how do SSNs relate to managing identity and what's the appropriate legislative or regulatory response? If folks are trying every vehicle they have and trying to fight fraud, there's a real question about do you make it harder or take tools away from organizations to fight fraud or not?

And, from our perspective, we think that people should assume that the SSN is widely available and

efforts to restrict access to it might actually create the obverse or negative consequence because people will think it's actually a secure number and they'll put more reliance on it. So, legislation and regulation to restrict access to SSN could have the opposite consequence of actually making people more reliant on a number that's outdated.

MR. CANTOR: Well, I wouldn't comment on any legislative or regulatory initiative of Congress or another agency. I will point out that one of the drivers, I touched on it briefly during my opening presentation, the consent-based Social Security Number Verification Service, the driver behind that actually is not largely a commercial driver. The driver behind that actually is a lot of demand from individuals. They all sign a consent form and they're coming into our bricks-and-mortar structures and saying, I want you to release the verification of my number to my employer or company X, I'm applying for a job, and all of these different transactions.

And a recognition that we don't have the resources in these times of limited resources as an agency to do that and realizing that there are other ways to do that and, basically, building a fully reimbursable system that would process that workload and take it out

of that structure. Because there's such a demand actually coming from individuals that they want their number, basically, demystified to that organization. Here, you tell them, you tell them it's the real one.

But one of the issues that we've always had is, where does that get you? If the entity assumed it was true to begin with, now they just know it's true. But that still doesn't mean you are who you say you are because, of course, you could be lying and saying, I'm Jennifer Barrett and here's my Social Security number and how do you know any better? So, you still need to use those other things.

MS. BARRETT: I'd like to maybe pick up a little bit on a different angle of Tom's question about regulation. And that is that I think we've all kind of acknowledged in some form or fashion that using multiple factors and being less reliant on the SSN is a good strategy. However, we actually took one of the tools, even though it's still -- it's not a perfect identifier, but it's one other piece of data that if you haven't lost your wallet, it may be a little hard to get and that's your driver's license number.

The Federal and State Driver's Privacy Protection Acts restricted the use of driver's license number for certain industries and certain states don't

let you use it. So, even if you wanted to get it, you can't verify it with the issuing agency. And, so, as we think about this issue holistically and as we look for alternatives to SSN, I think we need to be making sure -- it's a little bit of what Tom's point was about restricting it. We've restricted driver's license in an effort to protect that information and protect the privacy of consumers, but we may have actually hurt ourselves by not getting the permitted uses of that information quite right.

MS. LEFKOVITZ: Speaking about these alternatives, are there distinctions that we can make between account opening and account access as far as the role of SSN? Could we say that it's always inappropriate to use the SSN in account access? But is it inappropriate, is it possible to get a way at this time in account opening or can we? Are there opportunities for government/private sector partnerships?

MR. FRENCH: I'll start off. From Bank of America's perspective, passwords are probably, you know, once we've authenticated you through our account opening process, with most existing customers, when they call in, we try to drive them to use a password, and if they don't have a password, we kind of steer toward mother's maiden name. But one of the things that we try to drive our

customers to is to use something that they only are aware of. The password is a key. I'd argue that most financial institutions try to steer their customers, when they're calling in, to use a password.

Through the online banking system, as I mentioned earlier, we have something called I guess "secure key," and when you get through that first level of authentication using your user name and password, there's a secure key identifier that asks you that question of what's your dog's name or what's your firstborn's name. So things that you wouldn't normally pop up or a criminal wouldn't necessarily know right away. And there's a plethora of questions that you can pick from.

So, I'd argue that moving away from Social Security number, from an existing customer perspective, is a good thing.

MR. CANTOR: I'd just like to add, the second part of your question is you had asked about partnering and things like that and Emily actually touched on that in her opening presentation and she's come back to it about the idea of federating identity.

There are multiple opportunities, in my view, opportunities that have sort of been unexplored by the private sector or by the public sector, which is this

notion of developing a really strong identity credential at an entity that has a reason to do it. Say it's a financial institution or an investment broker or something and then using that identity in other secure transactions that wouldn't necessarily have had the opportunity to establish that relationship with you yet. And that requires a great deal of trust not only amongst the individual and the account, the entity that has the account or the relationship, but also between organizations whether they're all private sector or private sector and government sector.

But it is an aspect of sort of identity in this era where I think that there is a lot of room for exploration, a lot of opportunity for public-private partnership or just private partnerships. It's just sort of a -- it's not a really strongly developed frontier yet, and I think it brings a lot of opportunities to leverage a lot of sunk costs already so that you do have something far more secure than something that just relies on a group of fairly well-known identifiers.

You can continue to lower your risk by doing some of these knowledge-based types of authentication schemes, but, in the end, it's much more helpful to find when you have had somebody with that signature card and some of those first party interactions where you have a

very high level of authentication at the beginning.

MS. LEFKOVITZ: Well, let me now open questions to the audience. We have one right here.

MR. BURKHARDT: Mr. Cantor, addressing your comments about maybe PINs or other forms of identification being shared across the sector, is that the type of thing where you would have, for instance, a PIN that might be opened or a PIN that might be identified at Trey's financial institution be useable, if you will, at five or six different financial entities, the customer might be doing business with, as well as down at the -- gosh, down at the shopping counter when the person is getting ready to submit a check and then that PIN would be changeable freely and would be then changed across all those entities?

MR. CANTOR: That's one way to do it. I mean, there are multiple models, I guess, in working with this notion of federated ID. One way to do it is because I walk into -- and I'll keep picking on Trey's bank because I do go to Trey's bank. But if I went to Trey's bank and I go and open an account and I do a signature card and they look at my driver's license and several other forms of identification as part of establishing me, they have a very high level of assurance. They've looked at lots of things, so they've credentialed me. So, I could use

that, you know, basically that I've established that account and I could have a PIN with them, but I could establish a new PIN with a new organization or I could use the same PIN. It would sort of be up to the customer.

But it's the fact of the reliance that Bank of America, in this example, has said I am who I say I am, or there is a very high degree, and it's a similar level of assurance transaction. Let's say it's another bank at a credit union or an investment account, then you can use that same level to rely on for similar risk transaction.

Now, if I am also a Department of Defense employee involved in national security systems, the financial relationship might not be secure enough and, so, I might need to do something more. And, so, you may have an even higher level of assurance for transactions at that level and for things like renting movies and things like that, it's a much lower level assurance and wouldn't require something along the lines of a bank relationship.

But there are concepts there that really haven't been fully explored either by the government or by private sector that really could, basically, I think, help protect consumers, help protect individuals and citizens from a lot of the risks of identity theft.

MS. LEFKOVITZ: And if you can also say your name and affiliation. Question right there.

MR. McCARTNEY: Jim McCartney with Bearing Point. A comment and a question. First, I think you're absolutely right, identity federation is a very valuable tool. But going with that, I think we need to make sure we're keeping in touch with the fact that the level of authentication needs to match the level of the transaction.

And I think that's one of the things, to answer your question, Naomi, I think we have a lot of problem where the level of transaction doesn't match the level of authentication required, and that's where a lot of people do get into trouble.

But my question's actually for Jennifer Barrett. We have a lot more information and the availability to analyze and develop that is really getting better. Would you see us going more to instead of a credit monitoring to a fraud monitoring? Because you talked about monitoring unusual behavior, do you see them developing an algorithm to be able to say, okay, I understand that action, whether it's medical, whether it's criminal or anything else, is not consistent with that person's background?

MS. BARRETT: I think in high-risk areas, high

fraud areas like medical, that may be what we want and it may be very valid to do. Medical identity theft is kind of a reasonably new thing in terms of becoming much more prevalent in the last three or four, maybe five years, than it was say 10 or 15 years ago, and it has horrible consequences, far beyond financial kinds of consequences that we end up with in financial fraud.

So, I do think that we will see analytics like Tom's company does on the application end and like all of the financial institutions do in the usage end. Even your telephone company now will tell you, if there's an aberrant long distance calling pattern, and call you up and say, does somebody have your calling card number? So, I think that's a natural progression, but I think it's going to take a while before we see that emerging because we need some history and some knowledge of what we're looking for. And it's hard to develop those kinds of things when you're talking about a small sample size.

MR. OSCHERWITZ: Just to make sure I understood the question. The question was related to are people already developing anomalous models for healthcare to look for fraud. The answer is yes, it's already occurring, but I'm not sure that's the question.

MS. BARRETT: In the use --

MR. McCARTNEY: In the healthcare area and

other areas.

MR. BLAKLEY: Hi, Bob Blakley from Burton Group. Question for Trey French. You said that prevention of identity theft and fraud losses associated with that is a competitive advantage for Bank of America. My presumption would be on that basis that if another financial institution wanted to learn your experience of what measures are most effective at reducing identity fraud and if they wanted to learn, in particular, your most effective techniques, you would not only not tell them that but would actively work to prevent them from learning that, would that be true or false?

MR. FRENCH: Oh, I don't think we would actively work to prevent them from learning anything that would help them prevent identity theft. What I will say is that banking organizations work with their regulators all the time on improving their fraud measures, improving their measures in preventing identity theft. So, the same opportunities that Bank of America has, other financial institutions have. And regulators continually look at how we protect consumer information.

We're all required to have privacy policies, we're all required to have safeguarding information policies. All financial institutions have to have appropriate customer identification procedures in place.

Some are better than others. Those entities that have issues, you may not see that noted in the press because that's something that is proprietary and between the regulator and that financial institution unless it's something that's deemed so poor it's publicized through a written agreement.

What I will say is that we work with the folks up here Acxiom, others, Deloitte, and have that same opportunity that other financial institutions have to improve. And I think that if you want to grow as a financial institution in this environment, you have to protect consumer information. And if you're not going to do that, you're going to lose out in the long-term in seeing consistent revenue growth.

MS. LEFKOVITZ: I'm going to jump in here with a question because this has been sort of bugging me today. So, I look at the CIP or the Customer Identification Program and one way to comply with that is to match the information that you collect with a consumer report or something. While I've always sort of questioned how far that might get you if the person has provided perfect information, when we go back to this morning's conversation about synthetic identity theft, that should seem to weed out mismatched information. You can see now why I'm confused, right?

MR. OSCHERWITZ: Sort of a short history of synthetic identity theft, one of the things that happened with synthetic identity theft is people gradually build out a record. So, they might go through a secured credit card first or through other types of vendors and, at some point, one of those secure creditors will report to the credit bureau and they build up their dossier such that the information that will be checked from a third party will be information that they actually provided. So, one of the problems in synthetic identity theft is that the information that you check from external sources is information provided by the synthetic fraudsters.

MS. GIVENS: Well, I guess just to ask my question again, why isn't synthetic identity fraud essentially stopped at the first instance of it? It just seems like this is so obvious that this is a very thin file, I mean, this made-up person has probably a very thin file. A credit issuer, I would think, would not be in its right mind to extend credit based on such a profile. Really, I ask the same question, why does it happen, period? Do you have an answer? Go ahead.

MR. OSCHERWITZ: What I can say, and there's people here who are probably far more expert than me and I invite them to speak, but I think -- this is actually not my field of business, but one of the challenges when

granting credit is you have people who are coming to the credit system who might not have a credit record, they could be an immigrant into the country, they could be somebody who just graduated from college, there could be a variety of reasons why a person may not have a record. And how do you allow for a system where legitimate folks can get into the credit system and weed out the synthetic fraudsters?

I don't think it's an entirely simple issue. But people in the field can probably answer that better than I can.

MR. CLAWSON: I'm Pat Clawson, the investigative reporter and private investigator from Washington and from Michigan.

I'll tell you why we have this problem. It's very simple for somebody who has toiled in this vineyard for a long, long time. The problem that we have is the fact that the SSN is being used for authenticating transactions and the SSN was never meant to be an authenticator device, all right? The reason why we continue to have these problems, frankly, is because most of these folks from the financial industry are too damned cheap to clean up their act. They've placed the buck of expediency ahead of the buck of prevention.

As an investigator, I deal with banks on fraud

losses all the time. And I will tell you they're more than happy to eat the losses in many cases because it's just not worth their time or their trouble to go through it.

The other problem you have at a striking number of your institutions is you have some colossal morons making credit decisions. That's an issue that the banking industry has to deal with. Need I say more? Take a look at the home mortgage crisis for today's best example of that, and what's going on with credit cards, which is the next big thing to implode.

If we want to stop identity theft, it's very, very simple to do it. It's not a matter of restricting access to Social Security numbers. It's forcing you all from the major financial institutions to get on the stick and clean up your act because you've been too delinquent, too deficient for too damn long. That's the problem.

MS. GIVENS: You know, I don't know if I would call it morons but I think a lot of the computers are making the decision. I read I think when ID Analytics opened up its doors, and I'm from San Diego, ID Analytics is in San Diego as well, so I've had a chance to visit their operation and this is not a commercial. But when they opened up their doors, there was quite a long newspaper article in the "Union Tribune" just about the

whole issue -- first of all, that this company was opening its doors in San Diego and then they went into more of an examination of what's going on. I could not believe what I read. But I think they said it's something like 10,000 credit applications are processed every hour. Obviously, humans are not involved.

And I think maybe those morons that you're talking about are the computers and the algorithms behind those computer-generated decisions.

MR. FRENCH: I'll respond on behalf of the financial institutions, us morons. Just to say Beth's absolutely right. We approve, I'd say, about 14 million just credit card applications annually. So, what that means, let's say you're looking at an approval rate of probably 30 percent, you're probably talking about, you know, my math isn't great, around 40 something million applications coming through the system. That's a lot of credit applications that people are reviewing every day.

In not all cases -- in most cases, that's through an automated process, you're absolutely right. Now, our automated processes take into account a lot of the things that we talked about today. You know, we look at if there are multiple addresses tied to the same Social Security number, if multiple phone numbers are tied to a common fraud at -- their fraud phone numbers,

their fraud addresses, we look at all those things.

Bottom line, fraud losses hurt our revenue and to say anything other than that it just not true. The bottom line, it hurts our revenue stream. And to the extent that we can prevent fraud losses and to the extent we can prevent ID theft, we work very hard to do that, I'll just say that.

MR. CLAWSON: Just speaking from experience, okay? I've been around the banking industry, I've dealt with this kind of stuff for about 30 years. I think I have a little bit of perspective here, okay? The problem that you've got here is that you had a lot of morons in the form of young MBAs who felt that they could completely automate all loan processing. And, so, you have credit decisions being based on credit reports. The average credit report's got some errors in it. I mean, I've heard numbers that as much as 30 to 40 percent of all credit reports out there on the market have serious errors in them. You've automated the process so much you've taken the human element out of that. That was a decision made by people, and now you are reaping the sorry benefits of that process.

The financial industry can stop identity theft in this country almost overnight by adding different authenticators to the process and not relying solely on

the SSN. My bank here in Virginia recently was bought, all right? The new bank, and I'll name it, United Bank, which owns my former bank now, has got a telephone banking system. Guess what I need to punch in to get access to my account? Guess what series of digits I have to enter to get access to my account? That wasn't the way it was before, but that's the way it is now and that, my friend, is truly the mark of a moron in the banking industry.

MS. MOSSBURG: I want to comment on the use of SSN as an authenticator and the fact that it wasn't designed to be an authenticator, and I think that's absolutely correct. And I think that it has evolved into a authenticator and it wasn't set up with the appropriate safeguards and protections around SSN. It became used more and more and more and is more available to more people. But it wasn't set up as an authentication system and wasn't there for a protective as an authentication system.

So, as we move ahead and determine what we're going to use to authenticate, we just need to make sure everybody understands the rules upfront. It’s an authentication system we're putting in place and there are certain protections that need to be put around the credentials in order for them to be maintained.

Otherwise, if we just move to something else, if we move to driver's license number or some other number, we'll be having this same discussion in five years.

MR. CANTOR: Yeah, I absolutely agree with that and that was one of the reasons I went through, during my presentation, the story of how SSNs work and where they came from is because it's easy to repeat that because there is a lot of desire to look for something easy. But at the same point in time, whatever system you move to, you have to build proper safeguards around it for it being used in that capacity.

MR. HOOFNAGLE: This is a great panel and thank you all very much. My question is for Jennifer. I really liked your presentation, particularly the slide where you had scores attached to individual's applications. So, I have a couple questions around that.

Does Acxiom make a recommendation whether or not to lend credit when you make that score? I see that it said -- I think it said probably not or probably, you know --

MS. BARRETT: It's purely a confidence is the person is who they claim to be. It has nothing to do what they're applying for. In fact, it's probably used more widely outside financial services and credit than it

is in it inside.

MR. HOOFNAGLE: That's fair enough. Do you ever get feedback from your users on whether or not they do grant an account or do authenticate based on that number? I guess my overall point here is that there's a number of choke points where we can learn more about the crime and see what works and what doesn't work and we have the big red flag guidelines coming and this is -- you know, tools like yours are ones that give us the opportunity to tell whether or not more matching works, how much works, how much doesn't. To the extent possible, I'd really encourage you to share that data with the FTC because it really could show whether or not the red flag guidelines work or not and whether we need new ones or different ones.

MS. BARRETT: Thank you. We'd be happy to talk to them about it. Again, like I said, financial services, where it's used in financial services is really to decide whether or not to go pull a credit report or not because some of it is a cost decision. The authentication service we offer is a lot less expensive to say, don't go pull a credit report, you're going to come back with bad data or you're not going to even get one than it is to try to pull the report and pay for that activity.

But it is used actually more widely in non-financial services sectors and we'd be happy to see what -- we don't know what the decision -- we know what the answer is, the answer is we gave, we don't know what the decision is that the customer then makes with the answer that we give them because that's their either credit decision or account open decision or if it's in the case of an employment screening, employment decision.

But we could certainly look at, particularly, the lower scores and see what are the patterns, why do people get low scores and so on.

MR. RIDINGS: Hi, I'm David Ridings from Namesake Corporation. I appreciate the panel being here today, I don't think there's a moron in the bunch. Anybody that takes two days of their time to come up here and talk about this problem that's reached epidemic proportions deserves that.

What I do think, though, is I'm in the camp that believes that, well, we didn't get here overnight and it's not going to be fixed overnight. I understand the theory behind coming up with a different number. But I'm also in the camp of believing that if you empower the people to have control over their own credit reports and their information and empower them to protect themselves, they're going to do a better job at doing that.

Let me ask you, Mr. French, what does Bank of America do if you run across a fraud alert, for instance, that a victim has placed with the phone number on it and you have the person sitting in your office? Do you call the number or what exactly does Bank of America do in that situation?

MR. FRENCH: I'll talk generally about fraud alerts, how we react to fraud alerts in general. Whenever there's an alert, and the credit bureaus have many different ones, the one issue everyone is talking about is one that requires you to pick up the phone and contact somebody to make sure that it's them applying for the credit. We are going to take that extra step to do that.

Through automated processes, one of the things we talked about is a lot of the application systems are all automated. Well, one of the things that you should do, as a financial institution, is purchase the extra things that the credit bureaus have out there to pick up on those exact alerts. Bank of America does that. Those applications get kicked out. A representative then looks at that and picks up on the fact that we have to pick up the phone number and contact that customer before we approve that application. So, in all those instances, we're not going to move forward with the application

process until we talk to that person, verify the additional pieces of information necessary that are on the bureau.

So, again, we're not just going off the address, Social Security number, we're looking at the bureau, we're asking them to help verify some of the information that's there, and then we're moving forward with the credit application. So, in that instance, we're not going to move forward without going that extra step.

MS. LEFKOVITZ: Has that been helpful? Trey?

MR. FRENCH: Well, that's something we've always been doing. So, the ability to putting a security alert on your bureau has been there for a long time. Most financial institutions -- most customers have the ability or all customers have the ability to put a statement on your credit report that says, hey, call me if somebody applies for credit in my name. Well, we always take that extra step to do that.

All banks have access to that information because they can pay for the extra fee it costs to get that information. So, you know, if you want to take advantage of that, you can.

MS. LEFKOVITZ: Are there any other questions?

MR. BLAKLEY: I just wanted to defend the morons here for a minute because I think it's been a

great panel, and I wanted to say in response to the previous statement that authentication is really a terribly subtle and difficult problem, and the fact that we have it with respect to Social Security numbers does not mean necessarily that there's a single better thing that we can move to that will make authentication easier.

So, to simplify the discussion by saying that banks are morons because they use Social Security numbers to authenticate people, I think, is a gross over-simplification. They had to use something, it was available at the time and it has trouble now, but that doesn't mean that picking something else would have resulted in a better outcome today and that we wouldn't be here discussing this problem in some other form.

MS. GIVENS: I think that goes back to what a couple of us said, we shouldn't pick just one thing which, of course, the Social Security number has been. I do think that there's promise in multi-factor authentication systems. Just in doing the research for this panel, there's some very creative things being done and they don't involve the Social Security number at all.

MS. LEFKOVITZ: And on that note, I'm going to put a plug in for tomorrow because I think that we're

going to hear about all of the exciting things that are going on and talk about some recommendations about how we can move this forward. So, thank you very much to this panel. You took some heat and you really did an awesome job.

(Applause.)

MS. LEFKOVITZ: Thank you all, and we'll convene back here tomorrow at 8:45 a.m.

(Whereupon, at 5:00 p.m., the workshop was adjourned.)

C E R T I F I C A T I O N O F R E P O R T E R

MATTER NUMBER: P075414

CASE TITLE: SECURITY IN NUMBERS SSNS AND ID THEFT

DATE: DECEMBER 10, 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 2, 2008

FRANK QUINN

C E R T I F I C A T I O N O F P R O O F R E A D E R

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

ELIZABETH M. FARRELL