>> Rebecca Kuehn: Hi, good afternoon. We're here for our last and final panel of the day -- "Reclaiming the Future." We're looking at solutions going forward. My name is Rebecca Kuehn. I'm an assistant director with the Division of Privacy and Identity protection here at the FTC. And it's my pleasure to introduce, very briefly, our panelists. We have full bios in our folders, and because these guys are so impressive, we could be here all day if I read all their bios. So I'm just gonna give you a quick rundown of who they are. And our structure this afternoon will be a little bit different, as Mary Lou will tell you. First, to my immediate left, is Richard Hamp. Richard is the assistant attorney general for the state of Utah, was kind enough to come in all the way from there today. To his left is Diane Terry. She's from TransUnion. She's the senior director of consumer relations and fraud victim assistance. The next person is Tom Oscherwitz. He's from ID Analytics, He's their chief compliance and privacy officer. And then we have Jay Foley. Jay -- You may recognize the last name -- a little bit familiar -- from earlier panel. Jay is the executive director for the Identity Theft Resource Center, which is a nationwide nonprofit victim-service and advocacy program. And we also have Alan Simpson. Alan is the vice president of policy for Common Sense Media and has been involved in education on children and education issues. And finally, but definitely not least, Anne Wallace, who's the president of the Identity Theft Assistance Corporation, which is a nonprofit cooperation that operates ITAC, the Identity Theft Assistance Center. And without further ado, Mary Lou Leary, who you heard from this morning.

>> Mary Lou Leary: Hi. Good afternoon. It's amazing to see how many people are still here, even after you went outside at lunch. You're to be commended. You're really dedicated to this. And I see lot of folks in the audience that I know from my days as a prosecutor here with the U.S. Attorney's Office in D.C., my days at the Office of Justice Programs at DOJ, and my term as the executive director of the National Center for Victims of Crime, which is where I first learned about child identity theft, because we had a hotline, national hotline. And we got a call from a teenager whose father had stolen all of her information. Of course, there was a nasty divorce in the family, and she was trying to get loans to go to college. And it was a mess. And I thought, "Wow. This is incredible that a parent would do this." And little did I know it was just the tip of the iceberg. So, I'm happy that we have reached the point in this day where we're gonna be talking about going

forward. What would we say if we were in ideally equipped -- What would we say to a victim, say, a child victim of identity theft or the parents or guardians or whomever of a child victim? Would we have some real concrete advice to give that would actually prevent this from happening to other kids and would help this victim get his or her credit and life together again? So we're gonna take a little bit different approach to the panel today. Instead of formal serial presentations, we'd like to make this much more of a dialogue with our presenters and between the presenters and all of you. And especially, I think that's so important because we have so many folks in this audience who really know this issue and have been working on various aspects of it -- people from government, nonprofit, prosecutors' offices, victim advocates, investigators. So we really want to hear from you. Don't wait until the end to ask your questions or to speak up, because we're here to benefit from you-all as much as you are benefit from the panelists. For our folks who are viewing this as a webcast, you can submit your questions for possible consideration by the panel and others by e-mailing us at childIDtheft -- that's all one word -- childIDtheft@ftc.gov. So, I thought a good way to kick this off would be to ask Richard Hamp, who is from the office of the Utah Attorney General, to talk to us about a very innovative kind of partnership that the Utah Attorney General has developed to address this in their state. Richard, do you want to talk to us about how you-all are developing solutions?

>> Richard Hamp: Sure. Thank you. First, let's not mistake why I'm here. I'm not one of those brilliant people they were early addressing you about. I'm simply here because I'm annoyingly persistent. [Laughter]

>> Mary Lou Leary: It takes annoying persistence.

>> Richard Hamp: Thank you. Some years ago, I was tasked with writing the Utah credit-free statute, and in getting it passed, I ended up coming across a gentleman from TransUnion Credit Bureau, who is here, Eric Rosenberg. And, actually, we were diametrically opposed to each other through the credit-freeze process. But last year, I was approached by another representative in my state saying, "Hey, I'd like to do a child-credit-freeze statute." I thought, "Wow, that sounds easy enough." I went back to my credit-freeze statute, figured I could alter about one line and make it a child-credit-freeze statute and drafted up a bill. Then I started talking with some other states that I

know had done some child-credit-freeze statutes and called them and kind was comparing my language against theirs. And I forget, but one of the states finally said, "Hey, you know this only works if the kid has already been compromised and has a credit file open." I says, "Really? I kind of want to prevent it up front, rather than waiting till after. Why doesn't that work?" And they says, "Well, we don't know." And after several calls, someone finally said, "Why don't you call Linda Foley?" And I did. And I says, "Linda, how come, you know, child credit freeze is only limited to after the child's been compromised?" She says, "Well, I'm not sure either, but why don't you call Eric Rosenberg?" So now several years later, coming full circle, I'm calling up Eric and asking for his assistance. And I call up Eric and I say, "Yeah, this is Rich Hamp of the A.D.'s office." He says, "Yeah, I remember you." [Laughter] And I says, "Eric, I'm looking at doing a child-credit-freeze statute, but everybody is telling me it only works after the the child's credit's been compromised. How come?" And he says, "Well, the answer is very simple. It's we can't freeze something that doesn't exist yet." And I thought, "Well, that certainly makes sense." So I says, "Eric, we need to solve this problem. I have got thousands of kids in my state that have been compromised, and I want do something to protect them, but apparently, the process doesn't exist." And Eric says, "Tell you what. If you don't legislate me, I'll work out a deal with you. TransUnion will voluntarily cooperate with the A.D.'s office in coming up with a process." So I have to give Eric and TransUnion a lot of credit for something that was very innovative. Not only is it innovate because it's something new, but it's innovative because we've got government and private business cooperating to solve a problem that's unique to both of us. And, quite frankly, given the breadth of identity theft, this is the only way we're gonna get a handle on it. Government can't solve it all, industry can't solve it all, but together, we can probably come up with some pretty creative solutions. And the solution that Eric and I discussed and that has now evolved -- and we've gone through phase one -- is, in Utah, we have a very unique way of being able to identify child-identity-theft victims. In our state, Workforce Services maintains two data sets, at least two data sets. One is everybody who is employed in the state or unemployed in the state. And then they've also been tasked, because they have such a large data set, with also keeping track of people who are on some sort of public-assistance program. So if your child is receiving public assistance in Utah, it's in the same data sets that Workforce Services has. So this gives Workforce Services the unique ability to say, "Okay, I've got a kid here receiving public assistance who's 6 years old, but that kid is also reflected as a brick mason making $30,000 a year." And I have prosecuted a number of those cases

at this stage and can tell you -- I've got kids that are brick masons. I've got kids that are waitresses. I've got kids that are carpenters. And some of them are making better wages than what I am making, I have to admit. But nonetheless, we have a data set, and it's limited just to kids. We generally do 12 years or younger, because if the kids get much older than that, then they might legitimately have an income. But we can take a look at kids 12 years and younger who are receiving public assistance and determine if they're victims of identity theft, if the person misusing their number is also in our database, in other words, employed somewhere in the state. And so, when TransUnion and I first started this project, I ran three-quarters. In three work quarters of history, we picked up 700 kids under the age of 12 on public assistance who had been compromised. Somebody else was working on their Social Security number. We were then able to give that information to TransUnion, and TransUnion was able to structure a process and test it out. And I'm gonna let TransUnion talk more about their process, but essentially, what Utah has done is -- we've created a portal on our IRS Website where parents can come in and register their kids. We will check the parents' information through a verification system that exists already in Utah for voter registration online. We will then feed that information to TransUnion, along with the kid's information, with the fact that we've at least verified the parents' information. TransUnion then will have the ability to take the child's name and number and put it on their high-risk fraud alert. So if someone's attempting to open credit in that kid's name, there will be a message pinged back from TransUnion saying, "Check further. There may be a problem. This may be a minor's number." They're gonna be the choice of what message they send, and I'll let them talk about it, but the fact is -- for the first time, we will have a system where a message will be sent out, hopefully providing protection for the kid. The other thing that TransUnion's gonna do is -- they're going to suppress future credit histories that may come in or credit files that may come in on that kid's name and number once it's there and been checked by them. Now, what TransUnion can't do at this stage is suppress already-existing files without some verification of what the child's Social Security number is. And the question is -- how do we do that? Well, Social Security can do that, if we can get them to do it. Right now, they have their -- and they talked about it this morning -- a consent-based verification system. Terrific. The problem is it costs $5,000 to register and $5 a hit. Now, that's not too bad, really, except that the whole idea between TransUnion and the Utah Attorney General's Office was this program was supposed to be free, 'cause we all want to protect kids. We all think it ought to be free. I have to credit TransUnion. They have never once, in any discussion I've ever

had with them, ever suggested charging for this service. I don't want to charge for it. I don't even want to charge 5 bucks a hit. But the big problem comes is if we go down that ridge with Social Security, is I have to now develop programming, programming to collect the 5 bucks, programming to collect the parents' consent, programming to send all that to Social Security. And by the time even just the collecting 5 bucks and sending it to Social Security, I'm looking at $80,000 worth of programming costs. So, although the number doesn't sound very big, when you look at the developmental costs on my side, it becomes prohibitive. And so, what I've been trying to do is to get Social Security, their doors pried open, to say, "Hey, look, kids, our future. How about free?" And that's kind of where I'm at right now on that. The beauty of the program is, though, TransUnion right now can provide basically two-thirds of the protection. They can suppress future credit histories and they can send out right now with what we have. We're in the process of developing phase one, which will actually be an actual implementation of the program in Utah. We wrote our programming. We created our Website so that anybody can use it. Once we get the bugs worked out, get going forward, get TransUnion to the point where they feel comfortable, we're willing to open it nationally. All we want is some M.O.U.s from the various states saying they will verify the numbers they're sending us to send to TransUnion. But the whole idea is to start this out, work out bugs in Utah, then take it nationally.

>> Mary Lou Leary: Wow. That's impressive. Diane, do you want to tell us about how TransUnion operates in this whole initiative?

>> Diane Terry: Well, certainly. And it's an honor to be here, and thank you so much for inviting TransUnion to be part of this panel. Let me just start out with just maybe a little background to that. In TransUnion, we've been committed to assisting victims of identity theft and financial crimes, gosh, since the '70s, and more so in 1992, based on our experience and the fact that identity theft wasn't going away. We actually established a dedicated department to assist victims of this type of of crimes, including minors, even so far back. More recently, let's say, I think it was about 2005, we started, but 2006, we created an e-mail process to help parents and guardians determine, "Is there a credit file in my child's name?" And that was childIDtheft@transunion.com. And what that would allow a parent or guardian to do is to provide us with their child's information, and we would come back with a "yes" or a "no." In most cases, of course, it's, "No, there's no credit file,"

and, you know, that's the reassurance parents wanted to hear. In the "yes" situations, what we would do is ask the parents to provide us with proper identifying information so that we can confirm that we are dealing with the responsible party for that child. They would submit that, and once did, then we can give them the information that has been created, credit information that had been opened under the child's information. In 2008, we actually improved the process some. We actually created a secure form on the Website that made it a simpler process for the parents or guardians to check. And so, we've been working in the area of identity theft for quite a while and, really more in the past several years, focusing on minor and child identity theft. Before we started working with Richard -- And it's been a great relationship, and certainly he's really rallied to this cause and very creative in a solution. Last year, Joanne McNabb from California Protection of Privacy contacted us and said, "We have a law relating to foster youth, and could you assist us with that?" And we've been talking to Joanne for years and identity theft, as well, and working with her, finding a resolution for victims. This was something a little new to her and us at the time, and she said, "Would you mind doing a pilot for us and to help me look at the law with this pilot and see, does it need to be tweaked? Is this really what we want? And make some recommendation." We certainly did that. We supported that and worked with Joanne and provided her the information that she needed to help her with the foster-youth-identity-theft issue. After that, of course, then we've got some other states that we're working with -- Connecticut, as well. We have a process going with them, working with them. And, again, they've contacted us and said, "This is the solution we believe that we need in our state." And basically, we've talked it out and, you know, came up with a good program. And, like Richard said, you know, absolutely no charges involved. When we're dealing with identity theft and minors, you know, TransUnion has always believed that's the right thing to do -- to provide assistance. With Richard, what he's -- Basically, he pretty much covered it, I think, very well. But he's provided us with -- We're probably in phase one, right? Yeah, finish phase one and moving on. But provided us with a list that we ran and looked for Social Security numbers that were being used by others. And some, it appears, that they just picked that number out of the air, I mean, no intent to victimize a minor or anybody else, but they needed a number and picked one and started using it. And in a lot of cases, they then go out and not only get the job, but they move on further for credit purposes. So we were able to assist in that solution. And I think it's a very worthwhile process that we're involved in. Other than that, at TransUnion, of course, we've worked with Jay and Linda for years and other people in this group,

as well. In fact, Bo from Debix or Clear ID. AllClear ID came to us to and said the fairly same thing -- "I want to help minors and I want do this at no charge. I think that this is something that our company wants to do, AllClear ID. And, you know, will you work with us to in protecting minors?" And, again, no charge, you know? And we are working with AllClear ID in their free solution, as well. But TransUnion's been there working with minors for many years. I think, over the years, we've talked to hundreds of parents and guardians and, no doubt, through our e-mail address, thousands of, "No, there's not a file." And that's good news that we can tell them that so that they can, you know, feel free that -- or less concerned that the credit's an issue. Now, in listening to all of the panelists in the past, we know that credit's not the only issue. There's other things. And I can't talk to that, of course, but we do what we can certainly on the area of credit.

>> Mary Lou Leary: Really interesting partnership. Are you-all aware of any other partnerships or efforts to create these kinds of partnerships in other states?

>> Diane Terry: Are you talking to me again? I'm sorry.

>> Mary Lou Leary: I'm actually talking to you and to the audience as a whole.

>> Diane Terry: Well, I can tell you that there's several states that have contacted us, and again, we've developed, you know, different solutions for them relating to, you know, minor ID theft. Even before we were talking about the minor ID theft, the passport program through the A.G.s -- And I believe, years ago, Ohio contacted us, and we've been working with several of the states. And, again, some of that includes minor ID theft. But, you know, that partnership exists, and I think it's worked very well throughout the years. Started with Ohio. We are working with Illinois and some of the other states, as well.

>> Mary Lou Leary: That's great. Thank you. Tom Oscherwitz, from ID Analytics, has some research that's hot off the press that relates in a way to what we've been discussing here with Diane and Richard. So you want to share your groundbreaking news with us?

>> Tom Oscherwitz: Well, I certainly can attest that it's hot off the presses. We'll decide later if it is groundbreaking. Mary Lou, thank you for your question. First, I'd like to give tribute to Bo Holland of Debix. There already has been some research done in this space, and one thing at ID Analytics -- we're very concerned about raising the awareness of problems, trying to get as good a number as we can on the problem. So, over the last several months, we've been investigating an issue of child identity theft, and there's a couple different aspects of research that I'd like to show folks. First, about several weeks ago, ID Analytics did a study on identity manipulation, and what we did was -- we looked at our entire ID network, which has approximately 1.4 billion transactions. And it includes information on approximately 267 million Americans who are active in the credit space. And we tried to get a sense of to what degree is child identity theft or intergenerational identity theft occurring? And what we found was that about 2 million Americans, parents and children, are inappropriately sharing their identity information together. We don't know yet whether that sharing is kids stealing their parents', in terms of elder identity fraud, or the other way around, where parents are stealing kids'. And we also don't know whether people are 35 and 17 or 52 and 35, but we do know it's intergenerational. So from a larger framework, we do know that it looks like about 2 million intergenerational folks are sharing identity information. Now, to tackle specifically the problem of child identity theft, for about a year now, ID Analytics has been sort of providing technology now to six of the nation's top eight identity-monitoring services, something called the Consumer Notification Service. So, I'm gonna briefly talk about this, 'cause it gives backup for the research. What the service does is -- it connects credit issuers -- auto lenders, leading banks, leading wireless companies, utility companies -- directly with consumers. And what the service does is -- it tells the consumer if that their name, their address, their date a of birth or Social Security number is being used in the credit system. And if it is being used in the credit system, the consumer is alert, and then the consumer gets to say, "Is this or is this not me?" If it's not me, we help connect that consumer directly to the fraud departments of the credit issuers. So this whole network is sort of a consumer-credit-issuer network independent of the credit-reporting system. And we wanted to find out what we're seeing in the case of child identity theft. And further study, what we looked at were 172,000 children who are enrolled in this service over a 12-month period, between April 2010 and March 31, 2011. And what we found were 300 cases of fraud, confirmed as fraud by financial institutions. So this is what financial institutions call true fraud. And I want to distinguish this from other studies and also describe what it says and what it

doesn't say. This isn't looking at the legacy of fraud, so we're not talking about fraud that may have affected a minor five years ago or four years ago or three years ago. It's what fraud affected that minor during that period of time and what fraud was actually stopped during that period of time? Additionally, we also left out of the study information which would be we call errors, where there's information of a minor that's been connected with an adult, but it's not fraud-related. So we excluded all that information, as well. And we're also talking, as I said before, about stuff that's occurring real time. This is fraud that was actually prevented and stopped. And this is going to be a conservative number I'm about to tell folks, but it's a real number, and that is that by our best estimates, extrapolating from this data set of 172,000 folks, there are at least 142,000 identity frauds that are affecting minors in the United States each year, and these frauds actually are preventible. So, just to give folks a sense of that. A couple other quick stats here is that -- And this shouldn't be that surprising. Minors generally were less likely to get an alert from credit institutions about their information. It makes sense. Their information shouldn't actually be in institutions. But when they did get alerts, they were -- First of all, let me just say there were 16 times fewer alerts that minors received than adults. But when they did get alerts, they were seven times more likely to be victims of identity fraud. And I guess the last point I would make, just in terms of the highlights of the study, are that where did the alerts come from? 60% of the alerts came from the credit-card industry, and another significant percentage came from the wireless space. So that's what we're seeing. So, my comment here is that I think we are now getting some better visibility with this. And there's certainly more research to be done, but I don't think that the scope of a child ID theft is an unknown problem.

>> Rebecca Kuehn: Thank you, Tom. We really appreciate that. Linda? I think we've a mike coming around. Hold on.

>> Linda Foley: As sure as I'm sitting here, there are going to be parents out there listening on the webinar who will get this information via the media who are going to say, "Oh, I better check my child's credit report multiple times a year," even though we know children should not have a credit report. And we've been told that that causes a problem.

>> Rebecca Kuehn: Oh, now you're stealing my questions, Linda. Thank you. [Laughter]

>> Linda Foley: So that's my question. What do we tell parents? What do we do about parents who want to request credit reports four times a year? Because they're overreacting.

>> Mary Lou Leary: And, Linda, would you mind just identifying yourself and your affiliation with the ID Theft Resource Center?

>> Linda Foley: I'm the founder of the Identity Theft Resource Center. We're a nonprofit that helps victims across the nation without charge.

>> Mary Lou Leary: Thank you.

>> Linda Foley: And we do education, as well.

>> Rebecca Kuehn: Thanks, Linda. And as Linda's already pretty much asked my first question, we want to turn now to the credit-reporting system. What resources exist? We've heard this afternoon about pilot projects in Utah, pilot projects involving California, but we need to know what's available sort of more generally to the public. As we've heard that TransUnion has a process that a parent can at least find out if there is a file on a child, and so we've seen different recommendations what parents should do about checking. And so Linda's question is a good one. Is it the best idea to keep checking with the consumer-reporting agencies over and over again or does that even potentially create an issue for the parent or for the child?

>> Diane Terry: Well, as always, Linda does have the good questions. I can only talk for TransUnion. And when you say credit-reporting agencies -- But at TransUnion, if a parent goes to our childIDtheft@transunion.com, the process that we set up years ago, they're checking for a file. We do not create a file based on that check. So "yes" or "no." If it's a "no," we don't put that information into the system and create a file. And, in fact, we don't maintain files for children under 16 years of age. The problem there, of course, is the criminal -- I shouldn't say criminal. The person that uses the identifying information of a child typically is not going to give the birth date of the child, so they're going to make it appear that that Social is belonging to someone that is of age

and over 16 years of age. So that's the issue. Now, I know that we have Stuart Pratt here from CDIA that perhaps can talk about other reporting agencies. But, you know, I know, certainly, we're all dedicated to not maintaining reports on children.

>> Rebecca Kuehn: That's, I guess, a common part of the advice of people here is that there shouldn't be a file for your child.

>> Diane Terry: No.

>> Rebecca Kuehn: And all the three of the big three, as we call, them have information of way to contact them just to see if it is. But I guess the concern that has come out is -- and it sounds like you've addressed it -- whether or not just the process of checking somehow creates a file or creates an issue. Are there other procedures that should exist? Obviously, one of the challenges that we've heard discussed during the day is that, you know, things like the credit-reporting system -- until someone is a participant, the system will not have information about that child. And so Utah and TransUnion are trying. One particular approach is to just have a parent register. Are there other sources of information that, you know, can be used to sort of help determine if a child is in the system? Sorry. Stuart.

>> Stuart Pratt: I can't believe I have a microphone. That was a a big mistake to give me a microphone. So, a couple of things. First of all, I think Diane said it really well for the whole industry. Nobody wants a credit report on a minor. But all of our members, all of CDIA's members -- and, again, we represent over 200 companies that are in the data space. We probably touch 9 billion transactions in this country every year to help U.S. businesses manage risk and try to prevent identity theft from happening. So, with that, I'm really in line with what Richard said, and that is -- one of the greatest challenges we have, particularly with the the Social Security Administration moving to randomization of numbers, is that we'll have less of an ability to understand when a Social Security number is associated with somebody who's likely older or younger, because historically, understanding which ranges were active and which ones were not gave us some fraud- and security-prevention tools which we will not have. We'll have those tools for some time to come, because all those Social Security numbers don't go away that have been

built under the old system. But prospectively, we're going to have a problem that will continue to grow. We believe very, very strongly that the Social Security Administration has to find an easier system of access. And there have been fits and starts and efforts at this over the years, but I think all of our members would agree -- and we have a number of them here in the room, several of whom were on the panel today -- that it would be enormously beneficial if there was a trusted party relationship between the private sector and the government so that it would allow us to identify when any Social Security number is associated with a minor, whether they're part of a foster-care system or whether it's some sort of family fraud, as a couple of the different panels have discussed. So we think that is a critical dialogue that probably needs to restart, particularly because of the inception of this randomization process the Social Security Administration is kicking off. We think it is doable. We think the data security protocols are in place. Yes, there's always risks when dataflows, but the United States is built on the predicate that we are going to have a system of dataflows in this country that enable markets to work and to save positions and so on. So that's really important us. That would give must ways, by the way, to be more effective, even in terms of suppressing a file which is active on the system which is associated with a minor, for example.

>> Diane Terry: And, Stuart, instead of being more reactive, we could be proactive, if we could get this information. Much of the work that we do now is a victim calling us, where we're doing restoration, that type of thing. But this would allow us to be proactive and certainly enhance everything that we do at TransUnion.

>> Stuart Pratt: And I think for all of our members -- So I'll say it broadly, and then I see Tom wants to say something here, as well. All of our members also believe that we could build even more effective fraud-prevention and identity-verification tools if we had a real-time system of access or a different way to database the data, which would be the most proactive. I mean, the best solution is there never is a transaction that's flowing through the system that ties a minor's Social Security number to an adult's identifying information or there's some variation on the theme of synthetic identity. And, again, CDIA's members are the leading companies producing ID-verification tools, which prevent a lot of identity theft we just never see here when we have these discussions. But we can always do better, and one of the ways we can do better is if we could --

Again, because randomization, we're gonna have greater challenges going forward, and now's the time to probably begin some of that discussion.

>> Rebecca Kuehn: Tom?

>> Tom Oscherwitz: I would just say that one way to frame the discussion is to say that to solve the child-identity-theft problem, one way to solve it is to come up with a source of truth. When we look at child-identity information, historically, there hasn't been a source of truth for children outside in the private sector, because the credit system has been focusing on folks 18 or over or maybe 16 or over. An alternative approach is what I would call a monitoring approach. And we think about identity and the risks that the kids experience. It's typically not their whole identity, but constituent elements of their identity -- their Social Security number, a combination of their name and date of birth. So the other alternative of it is to create a way either proactively to monitor that information or to allow a child who has that information to say, "Please protect this particular elements of data." So, I just wanted to frame. At least that's the way I see the range of possibilities we have to protect kids' information.

>> Rebecca Kuehn: Well, let's turn to monitoring. Jay, you've worked with a lot of consumers, a lot of children. You know, is routine credit monitoring -- Are the forms of monitoring a helpful tool for parents who are trying to keep an eye on their children's information? Is it something that you've found useful?

>> Jay Foley: Credit-monitoring services are a viable and valuable tool for the parents to keep an eye on what's going on with themselves. It's not a tool that can be used by the child in any real way or fashion, because the information that's most likely to be in the system will be Social Security number and a different name. The only way we're going to be able to tie down the child-identity-theft problem is when the Social Security Administration has provided the Social Security numbers of everyone from zero to 17 years-plus to the CRAs for the purposes of, gee, a new application come in. The company wants to check this person's credit. There's no file. CRA goes back and says, "Oh, it shows up in the minor registry. You might want to rethink about that." It would be the perfect block. It would be easy to do. It would eliminate a lot of the pain, which is somebody

who's in a situation where their parents aren't the nicest people in the neighborhood or they've got a relative who's just as likely as not to steal their identity. They've already been blocked in that regards. Then all we've to deal with are some of the peripheral things, like criminal and medical identity theft.

>> Rebecca Kuehn: We heard this morning about other sort of forms of monitoring. We talked a little bit just now about credit monitoring, and obviously, in the absence of a credit file, it's hard to monitor what isn't supposed to be there. But are there other forms of monitoring -- and this really is an open question -- that are available? Will you please state your name and -- Thanks.

>> Mike Lamb: Hi, Mike Lamb from LexisNexis. And we don't offer minor monitoring, but we do have database with credit-header data, real-estate data, a whole array of data that you would think is associated with identities. And we're working with one of our partners who are actually gonna launch. Intersections is gonna launch something that, even though it's not gonna be perfect in terms of knowing ahead of time from the Social Security Administration what socials are a minor, if somebody uses that kind of a service, it looks for, "Is that Social showing up in any way, shape, or form? Is it showing up in utility files? Is the name and date of birth showing up in property records?" It's after the fact. I think the solution everyone's saying is to have something that prevents the misuse of identities ahead of time with greater authentication. But there is minor monitoring that, you know, companies are beginning to develop, including some people that we're providing data to.

>> Rebecca Kuehn: Stuart.

>> Stuart Pratt: So while the mike is close, I thought I'd grab it. You know, I'm just gonna sing from your own song sheet, Becky, and that's the Social Security report had that the FTC produced a few years ago. And so, we've talked around doing a good job of authentication. So we've already said we could do better. We could build even better tools if we had access to Social Security Administration data in a way that's real time. And I think, Jay, you described a very viable way that that could be done. But the flip side of it is utility companies and telecoms and everybody needs to do an excellent job of authenticating the identify in the first place. I don't know how many

times I've been in this room saying this same thing over the years, and that is -- how can somebody open up any kind of account with just a name and a Social on its own? Authentication should be much more than that. It has to be robust. We live in a complicated world. There are risks out there in that world. And this is true for adults as well as kids. So I think authentication tools -- those are things our members build. Those are datas that are available every day of the week. Red-flags rules even elevated the importance of those. U.S.A. Patriot Act, Section 326 elevated the importance of that. You hope you don't have to get to the point where other sectors of the U.S. economy have to have a U.S.A. Patriot Act, 326-like requirement before they get to the point of saying, "We will do really, really excellent authentication to make sure that we have tamped down on all of the front-end risks as much as we can.

>> Anne Wallace: Hey, Becky? Can I just jump on that? I'm Anne Wallace. And the Identity Theft Assistance Center is sponsored by the Financial Services Roundtable, so I'm here representing the financial-services industry. And I just want to give a big second to what Stuart just said. The financial-services industry knows how to authenticate people. It's true that, you know, the U.S.A. Patriot Act is sometimes burdensome, but let's face it -- it keeps the bad guys out. And the financial-services industry knows how to authenticate people. We know all about privacy and data security. And we feel very strongly that the protections that we have in the industry really should be applied to a lot of other industries across the board and really don't see the justification for picking and choosing, you know, among telecommunications and financial services and transportation and retailing. That's vital personal information in all of those sectors. And we're strong supporters of uniform national standards.

>> And one of the things we heard this morning was that identity thieves often will start with a smaller account or another account and sort of build that history, maybe not starting with the financial-services industry, but starting with other industries. And so the idea would be to sort of -- I don't want to say transfer, but apply those same standards beyond that, because it has a larger implication. One of the things that we heard this morning -- and anyone would like to comment on it -- was that once you get information in associating maybe the wrong person with a child's Social Security number -- Once it's in the system, it's much more difficult to get it out. And it's easier for that person to continue to use that information. Is that consistent with what your experience is?

>> Anne Wallace: I think that's right. I think any creditor would say that once the first line of credit is established, it is easier, you know, to get the next ones established.

>> Rebecca Kuehn: Mm-hmm. So, now you're a couple years down the road. Unfortunately, a child's Social Security number was compromised, accounts were opened. Jay and anyone else who wants to jump in on this one, we heard a little bit about this earlier. At what point should a parent or a child reaching the age of majority just say, "Well, my identity has been so compromised, my Social Security number has been used in so many places that I need a fresh start, that I need to go to the Social Security Administration and see if I can get a new number"?

>> Jay Foley: Usually, when we're dealing with situations like this, we're talking to a parent. Hopefully the child is somewhere around 16 years of age. Find out how bad the damages are, how widespread it is. At that point in time, now it's time to start the paperwork with the Social Security Administration to get the child a new Social Security number. Here's your 18th birthday. Here's your new Social Security number. Go forth and have fun. You're no longer tied to the previous number. Notify the necessary agencies and across the board that this other number had been used as fraud. And they can address it however they choose to. But that's where you would go for someone who is just coming up to 18. The problem in a lot of cases -- it's we are not going find out about the fraud until that nice little 18-year-old is actually applying for their first student loan. And now they're gonna spend roughly 12 months to two years trying to clean up this mess, waiting for their opportunity to get a loan so they can actually go to college.

>> Rebecca Kuehn: Should one of the recommendations be turn 16, get your driver's license, then check your credit report?

>> Jay Foley: Actually, that's the one we've made with the State of California. That's the reason for the basis of that law. If we could get to the children in the foster-care system before they turn 18, give us two years, a lot of that can be cleaned up, cleared up, and they can go out.

>> Rebecca Kuehn: And it sounds like it may be good advice for teenagers, whether they're in the foster-care system or not, just to see if there is information about them. And so we talk child ID theft, a lot about the credit-reporting system. Obviously, there are other areas were identity theft is occurring, such as employment and taxes. We've heard a lot about people using a child's Social Security number to secure employment when they may not otherwise have a Social Security number available. Are there any tools for prevention or remedies that can assist victims of that type of identity theft? And I open that up to anyone.

>> Diane Terry: I think it goes back, again, if we can get the verification that we need from the Social Security Administration. We could be more proactive, and absolutely, that would assist, that would enhance the process.

>> Rebecca Kuehn: Tom?

>> Tom Oscherwitz: I just, again, make a pitch for monitoring technologies. One of the challenges we said before with SSNs is that they could be all over the place. And so to the degree that technologies can be built to monitor the use of SSNs in various aspects of the environment, I think people have a better shot at correcting those errors, 'cause one of the challenges, of course, with credit reports, otherwise, is -- you have just synthetic identity fraud or that you have collections issues. And so the ability to somehow identify that misuse by the constituent-identity element, I think, is really a key to solving this problem.

>> Mary Lou Leary: I wonder if anybody here has ever worked with a victim or handled a case that involved identity theft outside of the credit-reporting system and what kind of challenges. Linda, what kind of challenges did you face?

>> Anne Wallace: If I could just jump in, because this is a really important point to us. The Identity Theft Assistance Center -- We've helped over almost 90,000 consumers recover from financially related identity theft. But our process, good as it is, is built around the credit report as it currently exists. So we can help victims of identity theft locate and start the recovery process with respect to financial fraud, but that's the limit of that recovery process. It's an excellent process, but

it's limited by the availability of the data. And so, we all know that there are lots of other data sources around the country dealing, you know, with medical records, insurance records, and all sorts of other things. And so, you know, one of the challenges that I think we all face is the lack of integration and the availability of a data so that you can do a complete recovery.

>> Mary Lou Leary: Good point. Jay?

>> Jay Foley: Areas in which we see identity theft touching children -- employment scams, employment situations. Somebody's working here. Somebody's working there. The notification usually comes to their parents when their parents' tax return is stopped up because you're claiming somebody who's working. We see this with parents who go into -- They go into a bank to open up a financial account for their child, a savings account, or maybe their child's first checking account, and they're stopped because of the financial information that wouldn't actually show up on a credit report. It's a bad-check situation. We see the criminal identity-theft issues, where somebody used a child's name, Social Security number, and now there's a felony record attached. It's matter of identifying, once again, the source of the information and going step by step to clear it up.

>> Rebecca Kuehn: I got a couple hands in the front.

>> Female Speaker: I think another one of the varieties of this is the healthcare identity theft, where unfortunately, once you've figured out the financial element, the insurance, and the billing element, because of some hospitals and some medical-care providers' interpretations of the HIPAA laws, they will not expunge the record. So they may put a note in the file that they will leave, you know, chronic alcoholism on a 6-year-old's file. That's problematic. And they believe that they are being compliant with other laws that they incompletely understand. So it's a much wider problem than financial in that aspect, as well.

>> Rebecca Kuehn: We have another gentleman right next to you. If you could identify yourself, please.

>> Tom Finneran: Yeah, my name's Tom Finneran, and my granddaughter was a victim, as has been discussed. But one of the answers that I thought from Ms. Foley's question about what do we do? We were told that the AllClear system addresses some of these things and would be good advice for the people and, you know, and it addresses beyond what, you know, the good work of TransUnion and their colleagues do. But it would seem to be one of the answers to the question was the AllClear system and anything, you know, like that.

>> Rebecca Kuehn: Thank you. Is there someone else?

>> Anne Wallace: There's a question way over there.

>> Keith Gethers: My name is Keith Gethers. I'm from Maryland Crime Victims' Resource Center and I'm a former supervisor of Financial Crime Unit in Prince George's County. And I'd like to thank all of the organizers and the panelists for your time. And we can tell that, obviously, there's lots of system-based kinds of things that need to be done, but what I'd like to try to shed some light on is the young people themselves and their activities that make them prone to being victims, and that is things like file sharing. That not only makes them prone, but also us, if we're using the same PCs, because once they engage in file sharing, then that computer then can be compromised. But also, the improper use of e-mails, social media, and things of the sort. So we can't get too hung up on what we can do and exclude them from this process in terms of making it better. So we have to be inclusionary with regards to bringing them in the fold and seeing what's going on with them and what they can help us do, because certainly, if there's a hint of some new technology coming out, they're some of the first people that's gonna find out about it and try it out. And oftentimes, it doesn't work out well.

>> Mary Lou Leary: That's really good point. Linda?

>> Linda Foley: On our Website -- and it's because we've been researching the Federal Trade Commission and another sites -- we do have a list of other types of specialty consumer reports that you can get. One would be about check fraud. Another one is on medical histories. Utilities is another one. So there are especially consumer reports, and because of FACTA, you are able to get

a copy for free once a year. And if you suspect that you're a victim, again, that same rule would apply, correct?

>> Rebecca Kuehn: That's right. [Laughter]

>> Linda Foley: She's my FTC approver.

>> Rebecca Kuehn: And just really quick, to follow up on the idea of children sharing information, little shameless self-promotion for the U.S. government, onguardonline.gov has a lot of resources for parents, including Net Cetera, which is how to raise sort of net-savvy kids, privacy-savvy kids. So it's a great place to look for how do you talk to your kids about what what information they should and maybe should not be sharing, file-sharing software, how it can impact your own security. So just a little plug for our stuff real quick.

>> Stuart Pratt: But isn't it really how you text your kids? You don't really talk to your kids.

>> Rebecca Kuehn: That's right. Stuart said it's how we text our kids rather than talking to them. [Laughter]

>> Tom Finneran: When the police officer raised that point -- The police do a great job, except in this area, I have been disappointed on a couple times. One is I was an adult identity-theft thing, which the credit guys helped solve the problem. But the bank recommended that I file with the police report, but my police department -- They said, "Please don't bother." And they gave me a big wad of papers that, you know, and while I'm a lawyer, I could figure it out, but when I read the bottom of it, it said, "Don't bother filing this police report." And then I saw on the "Today" show, where, you know, the guys track down two of the people who were felons. And the guy said, "Where are the cops? You know, handcuff me. Where are the cops?" There weren't the cops. Now, we know that the state of Arizona is now following up on that, 'cause we have -- Michelle talked to one of the investigators, so they're working on that. But how we can get the local and the feds to work together? To me, I would say that we need almost an FBI-type of unit that can help the various police to do this, because this is a federal crime. I mean, it's not --

>> Rebecca Kuehn: We have an answer from the audience. [Laughs]

>> Female Speaker: Probably not a good one. Probably not one that you want to hear. I struggled with the same thing, so I want him to know, as a victim, as someone that works for a state government, I feel the same frustrations.

>> Mary Lou Leary: Can you identify yourself?

>> Theresa Ronnebaum: Yes, Theresa Ronnebaum with the Florida Attorney General's Office, ID theft advocate.

>> Mary Lou Leary: Thank you.

>> Theresa Ronnebaum: Luckily, the state statute in Florida looked at that the and made some changes to the identity-theft law, which shows that the element of the crime can be where the victim resides or where any element of the crime took place. So we have tweaked it more towards victims' rights, but I still go through, you know, "Well, what's threshold of this agency versus state agency versus, you know, FBI or Homeland Security or ICE?" So I do want you to know that I think all of us, even dealing with the Foleys at a not-for-profit level versus an elected-official level -- we all feel that. But I think in time, if we had more manpower, then we might be able to address every issue. So a lot of times, it comes back full circle to collaborating and educating, because law enforcement cannot tackle this all themselves.

>>

>> Mary Lou Leary: And, you know --

>> Jay Foley: They are actually doing everything that they possibly can in most situations. Let's be honest -- who do you really want off the street? The guys with the pens or the guys with the gun?

>> Male Speaker: [Speaks inaudibly]

>> Jay Foley: Yeah, but the guys with the guns are likely to put a bullet in you and really ruin your day. Right now, we have a situation in California. In the prison system, they're going to let something like 40,000 prisoners go. The ones they're letting go are the ones who use their ink pens. They're keeping the ones that committed violent crimes. Law enforcement faces incredible challenges in identity theft, in investigating these cases and making a case and proving it. And one of the areas we were talking about earlier, the familial identity theft, rarely will you see a law-enforcement agency get involved in that because of the incredible amount of man-hours involved investigating it and the potential for it going to the point where it gets into a court of law and the victim says, "Well, maybe," and the entire case goes away.

>> Male Speaker: [Speaks inaudibly]

>> Jay Foley: There are a large number of law-enforcement officials in the U.S. right now working on the organized-crime aspect of identity theft. The problem we have is now, not only do we have jurisdictional issues within the U.S., but you have jurisdictional issues across the world. This is the only crime that I can think of where I can wake up and victimize somebody in Italy, somebody in Germany, somebody in Hawaii, and somebody in Japan. And I didn't even have to leave my house.

>> Mary Lou Leary: Yeah, there are incredible challenges, not just in person-power, but in training and sophistication, as well. So, you know, what is a victim to do? I'd like to just turn the discussion for a little bit toward, you know, other resources. What can folks in the nonprofit sector, in the education sector, in the advocacy sector, private sector -- What else can be done to help victims to prevent this crime or to protect themselves once they have been victimized and to move on and pull it together? I see a hand up over here.

>> Kayla Hall: I don't have an answer but a question along those lines.

>> Mary Lou Leary: And can you identify yourself, please?

>> Kayla Hall: Of course. My name is Kayla Hall, and I'm the coordinator for the Victims Resource Advocacy Program at the Department of State. And what we get involved with, crime victims in this arena, is through the visa and passport fraud system. So, often, our child victims obviously will become adult victims, and they have been taken away, their identity, by individuals who find a child looking similar to theirs and therefore take their identity. What we've seen as a problem related to resources is finding mechanisms to help beyond just the financial capacity that victims need rebuilding. And, oftentimes, identity-theft victims are not related as victims for victims-compensation programs, which has become a major problem. And we're not able to find mental-health services that help with counseling needs that these victims have. So if anyone could address resources beyond just repairing financially but building with those holistic issues that victims face after they have been changed for the rest of their lives in many cases.

>> Jay Foley: If you're dealing with a victim of identity theft in any area outside of financial, you can always turn to the Identity Theft Resource Center. We will assist every way we possibly can. The only limitation I put on that is -- right now, we're sticking to U.S. citizens, so...

>> Rebecca Kuehn: Over here.

>> Female Speaker: I think as an advocate, whether it's a legal or a state advocate, what you have to do is set the person up in the right mind-set to begin with. If their goal is restoring their good name and not in catching a criminal -- because you're not gonna catch that criminal, and even if you do, there probably will be very little sentencing going on. So you have to let them know from the very beginning, "Our goal is to restore your good name so that you can move on with your life and then put it behind you."

>> Rebecca Kuehn: Right behind you.

>> Ryan Martin: Hi, my name's Ryan Martin. I'm with the House Ways and Means Committee. And I have kind of a little bit of a different angle interest on this. As you may know Representative

Stark and Representative Langevin, last year in prior sessions, have introduced a bill about foster youth and ID theft. And I've been kind of looking into this issue to understand better, so I'm kind of a little bit in a different mind-set here looking at the child-welfare side. But jumping way back to Richard and Diane, one of the things you mentioned you started looking at was sort of a child security freeze. And it sounds like you're more looking at sort of this fraud alerts or kind of notifications. I'm sure there's a story there. Is there a reason that you decided to go more that route versus sort of creating a file and freezing that data until the children are older?

>> Richard Hamp: Well, yeah, there a couple reasons. One is -- what I'm trying to do is proactively prevent it, and since there is no file, there should nobody credit history. There's nothing to freeze. Now, to take and have TransUnion create a file just to freeze it, we're doing kind of two things. One is -- we're causing a private company, whose business model is really to provide credit scoring to other companies -- We're trying to alter their business model. I don't think that's fair to them. Whoop. Sorry about that. I don't think that's fair to them to alter their business model. But the second thing that we're also headed down the road there is collecting data on kids in order to create a file, and that's part of what we're trying to prevent is collecting all this data that everybody's collecting and then losing and collecting and losing. If we can kind of prevent that up front, we'll solve both problems.

>> Alan Simpson: And I think that's an important part in terms of -- You know, we've focused mostly on financial ID here, but we've also raised the point that there are a lot of other forms of ID. There are a lot of other forms of kids' data that's out there that is being collected. Some of it's being stolen. Some of it's being used for other purposes. And with all the limits that have been expressed about police power and that the limited opportunities for resolving these issues for victims once it's happened, I think we need to also remember how much more we need to focus on the prevention and the education around -- for kids themselves, for their parents, for others in their lives, about just generally being more careful with the information they have available online and they make available online. And it's very challenging. I think the Net Cetera resources are a great step in the right direction. I think there are other resources that's a large part of what Common Sense Media does in terms of tools for kids themselves. But if we don't start, at a very young age, teaching kids to be smart about their own information -- And we have to be very careful not to try to frighten

them away from the Internet and the great, cool, fantastic resources that are available to them now. This cannot be a danger notice as much as it has to be careful lessons that work for kids at their given age level. I mean, one of the ones I'm looking at for us is for grades 2 and 3 about just what is a password, so that kids learn early on to be safe and smart with their own information in the first place. Later, it'll become their financial information, but it's got to start long before that.

>> Russell Butler: Mary Lou -- And Russell Butler, Maryland Crime Victims' Resource Center. In addition to the answer about criminal injuries compensation, where a lot of the state programs just do not provide those mental-health benefits, the VOCA regulations don't allow for legal services for identity-theft victims. So, you know, we were very fortunate to get some burn money that does allow for that. And we've already been told by the state they're not gonna renew, and so it puts us in very much of a quandary as to how to keep providing these services, because the federal-funding streams, even though the money from VOCA, both for victim assistance and victim comp, come from financial fronts, a lot of that money doesn't go into those victim populations. So that's a big issue. Another issue is how to identify these victims and then, once you identify them, how you serve them. So, you know, you have a lot of technology, and that's how these crimes are being committed. You know, we need to use technology to identify those victims, notify those victims make sure that they're served. FTC has a wonderful pro bono book, but we got to get pro bono attorneys to use that. We've got to, you know, give it to them on a silver platter, use technology, make it easy for people to fill those out. So, you know, there are lots of things that could be done and brainstormed on how to build a better mousetrap using the incredible resources in this room of all that's being done technology-wise. And, you know, we've got to look at that not only in terms of prevention, but in terms of victim services.

>> Mary Lou Leary: Absolutely. You know, I do think, both as a former prosecutor and as a victim advocate at the National Center for Victims of Crime, that one of the issues that we face is that we know there won't be much by way of prosecution, and even if you get prosecution, you're not gonna get much by way of sentencing. That's not a very satisfactory route. However, I think we don't know enough and we don't do enough to educate the public about the impact of identity theft on a victim. You know, there was an expression when I was a baby prosecutor in the D.A.'s office, when all the police would come in for their intake, and people would sort of cynically say,

"Huh. No blood, no warrant." But, in fact, you know, that reveals a rather cynical view of victimization and what kinds of harm people actually suffer. And it can be very serious and long-lasting harm. And I think one of the educational challenges we have before us is to help the public and the policymakers and legislators understand that, that this is serious stuff, and do need funding, as you pointed out, Russell. You do need to amend those statutes and those regulations to allow for funding for victims' services. It goes way beyond just financial restitution. It's helping the victim deal with the emotional and sometimes the physical impact of that crime.

>> Rebecca Kuehn: Tom?

>> Tom Oscherwitz: Okay, sure. Just a quick point. When I think about identity-fraud-prevention efforts, you can put them into three buckets. One is increased enforcement, second is increased accountability and prevention by industry, and the third is the role of the consumer. I think, from my perspective, at least, one of the things that's a challenge in the child-identity-theft area is that a lot of the tools for consumers, which, in fact, are frequently the most powerful advocates and preventers of identity fraud, just don't work the same way. So if you're talking about free annual reports, you're talking about fraud alerts, you're talking about getting access to information and records, it just doesn't quite work for kids the same way it does for adults. And part of this, we've never really thought about kids from an overarching perspective And I guess this is really not a solution, but I think it's the area where we need to focus on is, you know, from across the board, we need to figure out how to get consumers who aren't children or their representatives the tools to protect themselves. So, clearly, TransUnion is doing -- You talked about doing some excellent work there. There's monitoring technologies out there, but that's really, from an overarching level, both in the business and the government and the policy aspect, how do you give kids the same type of tools that adults have to protect themselves?

>> Rebecca Kuehn: Bo.

>> Bo Holland: I'm Bo Holland with Debix. One problem that we run into is the privacy of an identity that uses a Social Security number from a child but has someone else's name and someone else's birth date attached to it. So we run into privacy concerns around disclosing this information

to the parent. And so my question is -- once we've confirmed we have an identity-theft victim, we've confirmed that it is, in fact, fraud. So that much is known. There is any clarification that FTC, DOJ can provide in terms of what are companies allowed to do and not to do with that information? So, again, the scenario we run into -- we know it's fraud. We know we have a kid. The person, again, we can't tell is the one who needs to know the most, who cares the most, which is the parent. And we get blocked and blocked and blocked on, "Oh, we can't tell them that." And it's a really awkward situation to be telling a parent, you know, "You've got a problem. I can't tell you what it is and the bank's not gonna tell you what it is and the credit bureau's not gonna tell you what it is." And, you know, you end up in this very awkward conversation.

>> Richard Hamp: Can I start with at least the answer to that? At least In part, we had the same problem in Utah, and it wasn't private business. It was when workforce services was discovering that they had these two data streams and were able to determine that someone was basically a victim of identity theft. They popped into my office and says, "Hey, we've got a problem. We're identifying victims of identity theft, but our statute says we can't tell anybody." So I went to our legislature and basically drafted a law that said, "Yeah, they can tell someone." And so we passed legislation that basically says workforce service cannot only notify me as, law enforcement, but also send notice to the parents. As far as I know, Utah is the only state where the state is actually sending notice to people saying, "Hey, you may be a victim of identity theft." Now, do we give the parent all the information about the person stealing? No, we don't do that. They give that to me to prosecute. And, Mary Lou, I'm gonna say don't give up on prosecutors. We probably need some education, too. But I issue hundreds of warrants on identity-theft perpetrators, put quite a few in jail, a couple in prison. So the system, I admit, does not work as well on white-collar financial crimes as it does always on blue-collar, but it's getting there slowly.

>> Mary Lou Leary: Good four, Richard. I mean, a lot of it -- You can see that law enforcement's like any other constituency. Education goes a long way. Awareness goes a long way.

>> Rebecca Kuehn: We have a hand in the back.

>> Keith Gethers: Keith Gethers again, from Maryland Crime Victims' Resource Center, and I'm a former investigator. It brings us back around to the reporting process that we were talking about earlier. And I go to a lot of events like this, and I tell you -- the group that I see missing most of all is law enforcement. And we talk about a lot of solutions and problems and that sort of thing when I go to events like this and that involve them, even, and then, oftentimes, expect them do those kinds of things, carry those kinds of things out. But they have lots of competing interests. The focus is usually on crimes against persons. But with that being said, by the time we leave places like this and talk to legislators and that sort of thing and the laws changed or policies are changed, then you have law enforcement begrudgingly going out to take reports from victims. So officers have been desensitized to the problem, because the problem is everywhere, but what we need do is -- we need do need to include them so that they see the value in taking the reports so that it's done correctly, because the harm in that is officers are victimizing people by not going out and taking reports. And certainly, they should be taking those reports. The police case numbers are like gold to the victims to get the process started, but the other problem with that is -- until we acknowledge that problem and fix it and properly educate law-enforcement officers, then for every victim that goes through that, they're less likely to participate in the process in a productive way from that point on. And we do know that people are being revictimized over and over again./ So I think we need to address that piece with involving law enforcement. And, no, they're not going to make much headway with regards to the investigation of the crimes, but certainly, we have enough officers in this country to go out and take the reports and get it started.

>> Mary Lou Leary: That's a very good point. And the other point is that you can revictimize -- Even if you show up and you take a report, you can revictimize by the way you treat the victim.

>> Keith Gethers: Absolutely.

>> Mary Lou Leary: And research tells us that, oftentimes, law enforcement is the very first contact the victim will have, regardless of the nature of the crime. And if that law-enforcement officer treats the victim with respect, that's all we're asking -- civility, respect, take it seriously, and don't hold out, you know, false -- Don't present false hope to the victim, but just treat that victim with respect. It's kind of a head start on the road to recovery for the victim.

>> Keith Gethers: And what I found that worked best with regards to that is direct training for the officers. You have to have somebody to go in -- and somebody that they're going to respect with regards to training -- go in and do that training so that they can see the ramifications of the crime, explain to them that it could happen to them, it could happen to anyone in their families. And then there's a whole new appreciation right from the onset of that training session.

>> Rebecca Kuehn: I'd like to throw a quick question out to the panel first and then to anyone else who wants to challenge it. I see that we're quarter after, and I really want to sort of move forward. If you could sum it up, what's the best advice we can give parents today? And let's start at the end with Alan, if you don't mind.

>> Alan Simpson: Well, I'd connect this to, you know, some of the work that Common Sense Media has done recently about privacy generally for kids. And we tend to look at it as a simple two-part equation, and I think this applies to financial information and ID information, which is, as a parent, you can't protect your kid's privacy online, you can't protect your kid's financial information online unless you understand how the online world works. So we throw that back at the many parents who come to our site for information as, you know, "This is just part of Parenting 101 in 2011. And if that seems too complex, sorry. You need to learn how this world works. You need to find out more about problems like these so that they don't affect your family and you can do as much as you can to prevent them before they happen." The other part of the equation for us, again about privacy and everything else, is -- you can't protect your kid's privacy online unless the companies working in this space give you opportunities to do so. And I'm not throwing that at the financial community in this discussion we've been having. But in the broader environment, there's way too much that goes on, especially with kids' personal information, without permission from their parents and without enough opportunities that the Internet service providers, the social-networking companies, the various actors in that space could be doing a lot more to inform parents about why they need this information, whether you can decide not to use that information or share that information, and also just to educate parents in the first place. But I would say, for parents themself, you have to dive in. You have to learn more about what's going on in this space or you will be caught unaware.

>> Rebecca Kuehn: Jay?

>> Jay Foley: For parents, what we are always talking about is take the basic approach. When somebody asks for your kid's Social Security number, why do you need it? Who gets access to it? What steps do you take to protect it? And when you're done with it, how will you dispose of it? If they can't answer any one of those questions appropriately, don't share your information or your kid's information with them. Treat it just as valuable as it actually is, because it, in fact, is more valuable than anything else you happen to own.

>> Rebecca Kuehn: Thank you. Tom?

>> Tom Oscherwitz: Just a couple quick points. First of all, child ID theft is real, but don't panic. It's a problem that we're starting to get some visibility into. Second, to echo what some of the other speakers said, I think the advice you apply to general individuals applies here, too, which is three steps -- you know, be careful what you share, protect what you have, and monitor, monitor, monitor.

>> Rebecca Kuehn: Okay. Thank you. Diane?

>> Diane Terry: Well, they covered many ways to limit the risk, but maybe I would just like to add to it. There's been talk about the law-enforcement report, the police report, and that is a very powerful tool in identity theft, rather it be a minor or an adult victim. And I do understand the gentleman there. Years ago, you know, to file a police report on identity theft was near impossible. And there are still areas, depending on the resources available, where it is still a little difficult, but, you know, it is a law. And I think that it's very powerful and important that you insist on that report, because it will help in the future. Some individuals, some minors are revictimized, and to have that law-enforcement report is a very good tool to get their credit history restored, as well as working with any financial agency. The law sets certain requirements that we need to deal with that law-enforcement report, as well as the creditors. So I would say file that police report and stay on top of it. You know, limit the risk.

>> Rebecca Kuehn: That's really good advice. Richard, do you have anything from the state perspective?

>> Richard Hamp: Just briefly. One thing that I have noticed through my identity-theft prosecutions and the research I've looked at in my database is -- I've boiled it down. There's really two forms of identity theft -- that that you can detect and prevent and that that you cannot detect and prevent. And I think that parents in particular need to know that even though their kids have done everything appropriately online, that that themselves have done everything appropriately, not sharing their kid's information, their kids can still be victimized. And, indeed, in the majority of cases, I'm finding that kids are being victimized without anybody knowing.

>> Mary Lou Leary: Great. I think that's all really excellent advice. And, you know, I have two children myself, so I'm gonna take all of that to heart, particularly the, you know, educate yourself, be vigilant, and don't be afraid. Don't be afraid to say no when you're asked for your information or for your child's information. I think, as a society, we're kind of socialized not to refuse requests for information. Maybe, you know, a clerk in a shop or a grocery store or whatever might ask for that information. You get that request in all kinds of contexts, where it's really just not necessary. And it's important to ask and be very firm about not wanting to share that information. And empower your kids, just the same way you do when you empower them to say no to a stranger who says, "Hey, come on. I'll give you a ride." It's the same kind of thing.

>> Rebecca Kuehn: And so, turning that to the audience, if there were anybody that wanted to participate. You know, what is the best advice out there for parents or for people who work with victims of identity theft? We've a --

>> Female Speaker: Two things that we didn't mention that I will say I use frequently, which is the Federal Trade Commission's memo to police. Love it. When law enforcement kind of gives me that roadblock of, "You know, we really cannot provide a detailed police report. It's not a threshold. It's not an out-of-pocket loss." I've heard every excuse. Then my next ammo is to provide the parents or the victim with the version of the FTC's memo to police, and it works

wonders. It doesn't always get law enforcement to take that report, but that's one more thing that we have in our bag or, you know, our little bag of tricks, and it definitely assists. I see ic3.gov when I'm working with middle-aged to middle-school-aged children love the ic3.gov for the press-release section. That helps people understand, on the Internet, what type of current scams are going on, and that runs the gamut, whoever's using the Internet, be it a middle-aged person or child that's in middle school when we're out presenting. I think that really helps knowing our resources. So those are two that, offhand, I can think of.

>> Rebecca Kuehn: Stuart?

>> Stuart Pratt: It's a little off of the question, but I think it's really -- You've heard a lot of really good discussion. First of all, I think, Tom, you said it really well. We're still on the front end of learning enough about children's ID theft and some of the patterns and what goes into it. I would just say, for the sake of all of us who are watching and been here, now's not the time to try to lock in a very narrow legislative solution. You've heard a lot of good ideas. There's pilot tests that are going on. There's outreach that's going on. But to start to roll that into rigid laws may just allocate costs to an idea that doesn't work well at all now or that may not work well next year, because next year, we have a mobile-device issue, which is different than a static lender-transaction issue or a static issue with utilities, for example. So I think one thing that I'm walking away with is -- there's a lot of innovative though that's going on. There's some interesting public sector/private sector partnerships that have been emerging. We got to see how those things are working, continue working on those kinds of processes. I think we'll do a better job if there's market incentives out there. And there are market incentives out there, I think, to build these kinds of databases and integrate Social Security administration data and other kinds of data, if it can be made available.

>> Female Speaker: I'm putting my corporate hat back on. In a couple weeks, I'll be joining McAfee as its chief privacy officer, so this is based not on my advocacy hat but my corporate hat. As consumers, as parents, don't be afraid to tell the companies with whom you do business that you care about privacy. The popular press thinks that Facebook has decided for us that we no longer care about privacy, that it's now this just sort of free-flowing commodity that no one cares about. If you speak up and you let your voice be heard, corporations react to that voice. So to don't be

unempowered, don't be disenfranchised, and don't listen to the common thread that one or two companies have somehow subverted, you know, thousands of years of interactions between humans. So go back to those companies, especially if you're dealing with them on family vacations or resorts or hospitality or airlines, all of these sorts of places -- If they're collecting too much data that you're uncomfortable with, there's always a comment section on their Websites. Don't be afraid to use your voice. It's the strongest tool the internal privacy officer has to go and speak to her C.E.O. or other boards of directors who otherwise are looking for legislation as bumper guards. They'd rather bump against a consumer requirement than a piece of legislation any day of the week. So please feel very empowered.

>> Rebecca Kuehn: Good point.

>> Mary Lou Leary: Excellent advice.

>> Rebecca Kuehn: Linda?

>> Linda Foley: I'm sitting here and realizing there are still a lot of advocates who work with crime victims, through D.A.'s offices, through other areas that we have not touched upon yet and gotten this information out to. Any advocate that works with a child-abuse issue should be looking for child identity theft, as well. Anyone who sees that there is an addiction problem, a drug-trafficking problem, or drugs being used needs to be looking for child identity theft. And it covers a broad area. And it's true for adults, as well. You know, it's not just children whose identities are being used. There are adults who these drug addicts are going out and stealing out of their mailboxes. We need to do more networking. We need to have more collaborative efforts. And in an answer to the police-report thing, persistence pays off. I have climbed up many a police leader, and if I have to talk to the watch commander, I will. I'm not afraid. What's the worst they can do? Say no? Jay, I know, has a good story. In California, we do have a law that they have to take a police report. I'd love to see that in every state. And when they don't, the question is -- "Hmm, who do you hold responsible for not taking that police report? The police chief? Is that who goes to jail now? They violated the law?" We need more laws about mandatory taking of police reports. The FTC affidavit is strong, but it's still not a police report. And Diane's right. It's your

biggest tool that you can use. But we need to get more advocates out there working for kids, counselors in schools, who are aware of this, who can go and who can be the go-to person if a child realizes they've been a victim. There's a lot of people we need to reach out to still.

>> Rebecca Kuehn: Thank you so much. And one last question, then we need to wrap up.

>> Male Speaker: I'm sorry. I arrived a little bit late, so if this has already been covered, I apologize. But it seems in all 50 states, there's a patchwork of laws regarding credit freezes, and I think that's a very simple and easy solution is a patchwork, where you have a new child. You can freeze his credit until they grow up. You unfreeze it when they're 18. And already, certain states, it's legal to freeze. I'm from Washington state. I only get to freeze my credit after it's been abused. So it's sort of like after the horse is out of the barn, then I get to lock the barn. And then some other states, it's not legal to freeze. And I wish there was consistencies across the credit freeze laws, because it would at least give citizens some kind of a tool that they can access themselves. I Understand why credit agencies want to prevent that. It hurts their business model. But at some point, there has to be a trade-off between the two.

>> Rebecca Kuehn: Well, just to follow up on that fairly quickly. One of the things that we did discuss -- and I'm sorry you weren't here for it -- is that it's very difficult to freeze that which does not exist. And since most of -- We understand that credit-reporting agencies don't maintain files for children under a certain age. If there's no file to freeze, there's nothing to do that. The other thing that we're aware of -- and I'll save Stuart from chiming in again -- is that at least in all of the states, the three credit-reporting agencies have at least some form of a credit freeze available, whether the state has mandated it or not. They have the commercial available in every state. But with that, I'd like to wrap it up and thank our panelists and the audience, as well, for such a great discussion. Thank you. Thank you very much. [Applause] And without a break, 'cause we like to torture you late in the afternoon, we're gonna sum this up. And I would like to turn it over to Maneesha Mithal, who's the associate director of the Division of Privacy Identity Protection. Thank you. [Applause]

>> Maneesha Mithal: Thanks, Becky. Thanks, Mary Lou. I'm just gonna take a few minutes to wrap up what we heard today. I, first of all, would like to start by thanking everybody for their terrific participation, both to the panelists and the audience. I think you've made today a very productive and informative day of discussion. So, I thought I'd spend a few minutes just talking about how what we can take what we've learned today and translate it into some concrete action steps. One speaker this morning said that child identity theft is not just one person's or group's problem. It affects children, parents, school systems, governments, businesses, and, in fact, the whole credit-reporting system. So I think the solution should be one where we all bear some responsibility. So, on the prevention side, I see three main action items that I heard pretty repeatedly throughout the day. First, for businesses and credit bureaus -- better authentication methods. We've heard repeatedly that SSNs were not intended to be a national ID. Companies should look for additional ways to authenticate consumers and shouldn't rely solely on SSNs. At the same time, we know that one way in which credit bureaus authenticate us is to ask for pieces of information from our credit files. That might not be be an option for children, so we should work to find alternatives. Second, for businesses, schools, and other entities that collect children's information -- this was brought home on the final panel -- we need better data security. There's no reason that a Girl Scout troop or a Little League team needs a child's Social Security number. For those who do need it, like school systems, they should secure it. And when a child has graduated from elementary school, for example, I don't see any reason why the school needs to keep the child's Social Security number. So they should properly dispose of the Social Security numbers. Third, for parents and children, more education. Again, these are messages that we heard on the last panel. We need to teach parents to be skeptical when giving out their child's SSNs. They need to ask the Little League team or the Girl Scout troop why they need SSNs. And if they don't get a good reason, they shouldn't give it out. They should encourage their children not to give out too much information when they're online on social-networking sites and other places. Then turning to the victim-assistance side, I think there are also three action steps that I see here that emerged from today's discussions. So first, for businesses, lawyers, other advocates, we really need to continue our advocacy efforts. Today, we heard about struggles around ensuring that child identity theft is seen as more than just a paper problem. I think there are many advocates in this room that have done a great job of articulating the serious and ongoing harms that result from child identity theft, from economic harm to, in some cases, unfair incarceration. We need to continue to work to

educate the public. We need to work to educate local law enforcers, as well. Second, for young adults seeking credit and for parents who are helping them, I think there's a clear consensus that solutions that may help adults won't necessarily work for kids. We heard that checking credit reports only catches child identity theft 1% of the time. We heard that fraud alerts may not work. So we need to tell people what does work. Perhaps this is an issue we need to come together and do some education around. Third, for all of us, we need to continue to develop solutions. We heard about some of them today -- the Utah program, the AllClear ID initiative. But these solutions won't work overnight for all consumers. We need to pool our resources to do more education, both about the problems, as well as about the solutions. So that's a broad overview, I think, of the consensus points that emerged from today. If you'll indulge me, I just want to take a few minutes to thank some people who made this event happen. First, I want to thank Mary Lou Leary for her participation today and all of our partners at the Office of Victims for Crime at the Department of Justice. The people who have contributed enormously to this effort include Laura Ivkovich, Jaimee Napp, Bethany Case, and Brooke McQuade. I'd also like to mention some FTC folks by name. Steve Toporoff, Lisa Schifferle, Cheryl Thomas were the key FTC people who helped put this forum together. I'd also like to thank Chanel Boone, Matthew Smith, and Megan Cox for their assistance today. Thanks to all of you for your outstanding work. So, this is not the end of the dialogue. It's just the beginning. If you have any additional thoughts, comments, articles, other materials, questions, feel free to forward them to our e-mail box -- childIDtheft@ftc.gov. And, once again, thank you all for coming, and thanks for your contributions. Look forward to working with you in the future. [Applause]