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

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.

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

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

>> 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.)TJ0 -1.725 TD.0002 Tc-.0012 Tw[(I think we are now getting some)]TJ0 3.452 TD.0

copen of achiuldIDt thfat ishanunk nony poibl m

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

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

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

>> 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.

>> 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

>> 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.

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

"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 woteand .9)me way. So if you're talking about free annual

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

>> 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

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-

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

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.

solutiid Wl. ord thre'-, I thi,1% of th