FTC Identity Theft: Planning for the Future Conference
May 25, 2017
Segment 3
Transcript

AMY WANG: A garage, so we didn't have a lot of things initially. So when I think about it, what we do in health care-- my husband and I-- is we restore the identities of people's health through rehabilitation. And I think, as we're doing this, people were siphoning information out of us, which is just so ironic to us, I think.

So let's highlight how I got here. In December of 2015, we start to receive a multitude of credit cards in the mail. Some were denials of credit, some started to become credit card bills. And it was like little snowflakes came in.

And my husband would have to come home at night, and with each and every one-- because he's very meticulous about things-- he would call each number, and you can imagine the amount of time it takes trying to get through customer service to each phone number. And then we noticed the bills that came through, so Bloomingdale's, Macy's, over $25,000. Now this is at Christmas time, and unfortunately, it wasn't gifts for me. So it was really sad trying to untangle this at that time frame.

So next comes the fun part of the movie. In the beginning of January, we received a letter from the US postal service, and our address had been changed, unbeknownst to us. And I thought, oh, this is strange. This must be some weird mistake. And it just has our name, and it had the Wang family, and then on the other side, it doesn't say where your address is being changed to.

So I called a number right away, and I thought, OK, this isn't us. Well, that apparently wasn't the only thing I was supposed to do. We didn't get our mail, and we didn't get our mail, and so I called the number again. We still weren't getting our mail, so I went into the post office, and they said, well, we're going have to fill out this form. It's going to take 7 to 10 days. It has to go to Tampa.

And at this point, every day my husband would come home and say, where is the mail. So I say these criminals were either extremely crafty or very lucky in the frame that they chose, because as this rolled into January, they got all of our W-2s, tax forms, bank statements, credit card statements, you name it. It was the jackpot. And our kids' social security numbers that were on their savings accounts that they had-- everything during that month-- Christmas cards, Christmas presents, because it was the end of December.

And with the US postal service, when they send the change of address form, it's an automated response. So our retirement accounts, all of our utilities, everything had been changed. And we didn't know where.

So we think that perhaps the breach of this-- because people have asked us about this-- we had received a letter from Wells Fargo at one point in time that said our information had been released. And also we received information that my husband's employer, through their employee

health, some information had been divulged. We put our alert on our credit agencies. And even at one time, I thought about what Ken said.

Macy's had even called and said, hey, we have somebody here saying that they're Michael Wang, and is that you. They were trying to make all these charges. And it wasn't. And we said, can you get security, and they said, no, we can only deny the charge. That's it. And I thought, what a lost opportunity.

I think these aren't the only things, unfortunately, that have happened to us. We've had our credit card skimmed. We've had funds moved directly from our account. We've had a student loan that somebody tried to open up in my name. It feels like this endless battle for us. I think it's a little bit like cancer cells. People say, well, do you think this issue is resolved. And I don't think it's ever going to be resolved-- now especially that they have our children's information. I think it's especially tragic.

And the amount of time-- did it cost us money? Yes, it cost us money in terms of credit card and utility payments that were late, because we weren't getting our information. It especially cost us time and energy that we could have spent in other ways-- my husband could have spent in patient care, we could have spent with our children.

So I guess for me today, I hope that all of you that are here today, I know you have some vested interests in identity theft, and I hope that you can help other people like me and make a difference in their future. Thank you.

LISA SCHIFFERLE: Thank you so much, Amy, for sharing that story. That really is a very interesting face to identity theft. A really nicely told story and it includes all different aspects of identity theft-- child ID theft, tax ID theft, credit card ID theft. You said even your Christmas presents were rerouted and your mail rerouted.

So just to put that story in context now, we're going to hear from Tammy Fine from the US Attorney's office in Maryland. And she's going to tell us more about the different types of ID theft and the parade of horribles that we call it.

TAMERA FINE: Good afternoon. I'm also a federal employee, so I have to say that these opinions I express today are mine and not those of the Department of Justice. So when I look at victims, when victims call me, what I try to analyze is what dangers they're facing from the identity theft that I'm prosecuting or investigating.

And those dangers flow directly from the uses that are being made of the identities. There can be an enormous variance in the amount of harm to a victim, depending on whether their credit card was skimmed at a restaurant-- and it can be resolved by simply canceling the card and getting a new one-- or whether their identity is used in a pervasive way, the way the Wang's identities were used.

So we generally know, based upon the various statistics that the Bureau of Justice Statistics has put out, what harms are awaiting each type of victim. But we also have to remember-- and I

always try to remind myself of this-- that the person who's on the phone with you or the person who's actually experiencing it may be one of the 4% who don't get to resolve this problem with just a month's worth of effort. So there are variances, and we have to be aware that there are people who are unlucky enough to have lasting sustained harm from something that other people can resolve fairly quickly.

So first, we typically-- often-- default to thinking about financial fraud when we look at identity theft. And financial fraud is, again, a situation where you have wide variances in the harms that await victims of identity theft. Account takeovers are some of the easiest identity theft cases for victims to recover from. And that because there is a broad history on the account, and that history maintains things like someone called in, and authenticated them, and ask themselves as a customer, and changed the address. You can identify when the fraud occurred. You can identify when the new debit card was sent out, and you can track the fraud in that way.

That's not true in new account fraud, when someone walks into the Best Buy and opens an instant credit account, for example. The Best Buy doesn't have a history of what you've purchased in the past to compare the new purchases against. The individual typically in an instant credit scheme is going to burn through that credit before the credit card can reach the actual consumer, the victim in the case.

And so you don't have any changes of address. You don't have any of those things that would alert the credit issuer that this is in fact identity fraud. And it's much more difficult, and we see that in the statistics in terms of how long it takes people to resolve these issues.

Believe it or not, utilities and services such as that are among the most difficult ones to resolve. I have people who-- not to pick on the utility in the Baltimore area where I work-- we have a lot of trouble with BG&E in particular, because they refuse to note that our victims are victims of identity theft. And so we have people who can't get utilities turned on, because there's this huge bill that somebody else ran up in another address. And those are real harms that await our victims. We've had a hard time resolving those.

There are groups that specifically target not credit, but your actual bank account. The Felony Lane Gang withdraws money from your bank account. That's a much more substantial harm than losing access to credit is, which can usually be resolved quickly.

We also have and have been talking today about benefits fraud. I think you've heard enough about stolen identity refund fraud, which is a real issue. And the fact that a victim may only be out their money, their expected refund, for a period of four months or six months really matters, if you're counting on that money for some reason.

But we also have unemployment-related identity theft, social security retirement and disability related identity theft. And these can truly cause tremendous problems, because they hit people at a point when they're economically very vulnerable. So suppose someone has gotten unemployment in my identity, and then I lose my job, and I try to get employment. And I can't, because I already have it. Well, I need it right then. That's the time that I need it, and it's very difficult to explain to a victim why they're not going to be able to get that resolved.

Similarly, if my social security income is diverted to an account in the Cayman Islands for two months, it may only be two months. But if I'm living paycheck to paycheck, if I'm living month to month, that two months is an eternity. And you also have the ancillary problem of people whose benefits are canceled entirely, because someone is reporting income in the identity of someone else who's on disability. And their disability payments get canceled, because they have more income than they're allowed to have. It's not their income. They're not getting that money. That's quite a problem.

You also have, obviously, the employment issues that I was just talking about. And any time you have a large immigrant population, you're probably going to have quite a few individuals who are purchasing identity documents for employment purposes. And that can result in the sorts of issues that we've been talking about.

And again, there are also collateral impacts. So sometimes people can't get a job, because they can't pass a security clearance. Sometimes they lose their security clearance and lose a job. Sometimes their credit isn't sufficient for them to get a job. We've talked before about medical identity theft. I don't think I need to cover that. But this is one of the real problems that's emerging, because in an emergency situation, when you come into an ER unconscious, having somebody else's blood type in your medical record can be a catastrophic problem.

I'd also like to just mention briefly about the use of identities in criminal conduct. There have been a couple references to this, but we have a lot of people who use identity information in order to create an identity that they can give to the police if they're stopped, because they have warrants in their own name. A lot of times because they have been engaged in illegal conduct. They're fingerprinted. Their identities are identified anyway.

And now that victim's identity becomes an alias-- an official alias-- of a criminal. And that's showing up with regard to what they need to do in terms of if they have background checks or employment checks of any kind. It can also result in people getting pulled over, getting arrested, and getting pulled off of airplanes. And we've had every one of those things happen.

And then the last thing I just wanted to mention was that we also have situations where individuals have driver's licenses in multiple names. And that can cause a lot of problems. Increasingly, we have centralized driver's licenses records and reciprocity agreements.

So even if someone is using my identity to get a driver's license, because they've been revoked or suspended in Tennessee, if Tennessee has a reciprocity agreement with Maryland, then my license is going to get revoked or suspended as well. And so when we look at victims, we have to look not just at the immediate consequences, but these downstream consequences that can be so devastating to our victims.

LISA SCHIFFERLE: Thank you, Tammy. That was a really great overview of the different types of identity theft and the harms that can come from being a victim of identity theft. Now we're going to hear from Eva Velasquez of ITRC about how some of these harms may affect people and what she's seeing in her practice in dealing with ID theft victims.

EVA VELASQUEZ: Good afternoon, everyone. Just in case you're not aware of the background of the ITRC, we are a nonprofit organization founded in 1999. Our mission is to help victims of identity theft and the resolution of their cases and to broaden public education and awareness in this space of identity theft, privacy scams, and fraud, and data breaches.

One of our signature pieces of research is our Aftermath study. And I think that it's really important to understand. We've talked about transactions here. We've talked about the victim, and data points, and the data that we're creating. And behind all of this, there is a real person. There is a person whose life is being adversely affected by this identity theft issue by, this data compromise issue.

And it really varies based on who they are, and what they're experiencing, and frankly what available resources they have. You can see from these quotes-- they're taken directly from that study-- that it can have a whole host of aftereffects. And it's not just financial.

I think we have a tendency-- that's an easy litmus test. We can measure harm in dollars. And that's a mistake. There's a lot of harm that goes much deeper than just the dollars. In the Aftermath study, where we are surveying the people that we helped the previous year, we go back to them, and we ask them a series of questions. Of course, we do ask them the standards about how long it has taken them to resolve their case, and how much money did they lose, or what other expenses they had. But we go much deeper.

And you can see there are a whole host of emotional reactions. Now, when you see that last one, the suicidal 8%, it may be hard to grasp that a financial crime such as this could cause such a strong reaction. But if you really listen to what Amy was saying-- and thank you again, Amy, for being here and telling your story-- this can be so frustrating. It can be so overwhelming. And feeling like you will never get out from under it, that it can cause those kinds of strong reactions.

In fact, we had a victim of medical identity theft who a drug addict had stolen her purse and presented her information to a hospital when she gave birth. And this victim is forever on the birth certificate of this unknown child, was investigated by CPS, because as the birth mother left the hospital, there was a child abandonment case. She was embarrassed. Her reputation suffered. Her children were questioned, and they were young and scared. So it did create a tremendous emotional reaction in her.

It goes even deeper-- behavioral and physical reactions. And if you're not compelled by the statistics about people being unable to concentrate, not sleep, or even go to work, if you think about that from a business case standpoint, that's a lot of lost productivity. And it's not affecting just the employer.

It's affecting all of the coworkers as well. If you have a coworker who's a real go-getter and somebody who's really pulling their weight, and all of a sudden they have a life altering event, and they're distracted and not getting things done, you tend to-- as a team, you'll pull together, pick up the slack. That's affecting everybody in that workplace.

And we think this is a really important principle to remember-- is that even though we are talking about and talking to individual victims, this really has a ripple effect, because it's not just their feelings and what they're doing with their case. It's also what they're not doing.

We've talked to folks who've had to put off life milestones, put off purchasing their dream house, put off school, educational opportunities. If you think about it with child identity theft, if that person-- that young person-- who's trying to launch has been unable to get student loans or even student aid, and they have to delay their education while they clean up their identity theft matter, whether it's a semester or even a full year, that is a semester or a year that they are behind their peers permanently. They will never get that opportunity back. How do we calculate that in dollars and cents? How do we calculate that lost opportunity cost?

And when I talk about that ripple effect, there were several actions when we asked the question of folks, if your identity theft case caused a financial gap, how did you bridge that gap? How did you meet that need? And we had a number of answers. Some were very creative. Some were very unique. But by and large, people were either borrowing money from family or friends, or they were requesting assistance from the government.

So this 17% that had to avail themselves of those government benefits, we can really trace that back. We can see how that affects us at the community, at the state level. And that's significant. But even the folks that were borrowing money from their family and friends, that is affecting you at a community level.

That is money that these people are using to help a crime victim that's not going back into your school, community school fundraiser, not going to the local businesses in that area. Well, I can't go out to dinner for my husband's birthday, because the money that I was going to use for that, I actually had to help my sister pay her rent, because her bank account was drained. That is affecting all of us.

So I would posit to you to consider that even if you weren't a victim of identity theft last year, you are being directly affected by it because of the responses to these questions. And I will just leave you with a few more of these quotes. These are directly from them. Don't take it from me. Take it from the victims themselves.

LISA SCHIFFERLE: Thanks so much, Eva. That was really, really interesting to hear about some of the effects that identity theft can have on victims from being investigated by CPS-- which is something I've never heard before and really very troubling-- to having to delay school, having to delay buying a house, and of course the emotional and suicidal thoughts that could accompany having to be put through these sort of life situations due to identity theft.

Now we're going to turn to Ellen Abbott from Kroll and hear some about what she is hearing and seeing from the identity theft victims that she works with.

ELLEN ABBOTT: All right, thanks, guys. And thank you, Amy, for coming here. It's hard as a victim to want to tell your story, especially to strangers who you don't know.

We talk to victims everyday at Kroll. I'm the manager of consumer investigations there, so I oversee a team of restoration investigators, who solely focus on the working victims cases. So our standard case, I would say, is around eight months on average for a couple of credit cards.

We've had chronic cases where a person is actually living as someone else in another state and continues to live and sometimes pay bills, sometimes not pay bills. And it just continues on and on, and we keep those cases open as long as we need to. But we've seen some go eight, 10 years.

And maybe they might subside a little bit or come back. We didn't pay another bill again. I got another call from a collection agency. Can you help me out? It's like, OK, here we go again. It's very frustrating.

Over the course of the time we've been in business, we've restored over 5,000 identities. So that's something I'm really proud of, something I'm really proud of with my team. We have a very experienced group of investigators who really, truly care about what happens to these victims, and they develop relationships with them. They get Christmas cards from them sometimes or gifts saying, you've helped me out so much. I enjoy seeing a victim going from victim to made whole, financially, emotionally, physically, and seeing that progress.

Some of our more interesting cases-- we've got some interesting cases going on right now with apartment fraud, where someone is living in an apartment. And the victim finds out through an inquiry that shows up on their credit report from a home rental, doing the background check. And the perpetrator may be paying rent, they may not be paying rent, and getting the leasing agent to go to that apartment and say, hey, knock on the door. You're not the person you said you were; you need to go.

There's one case where the apartment leasing manager was like, she's paying her rent, I'm not going to do anything about it. So that's put our victim at a disadvantage, because she lives in Minnesota and the perpetrator's in Georgia and has a fake South Carolina driver's license. So that one is a particularly difficult case.

We've caught one of the cases that I want to talk about as well, probably a more pervasive case. This one only took about two years to resolve, but it was probably the most interesting and convoluted situation. So our victim was in Louisiana.

She went to go renew her driver's license. The reciprocity said no, because there was a driver's license in Iowa that had moving violations on it-- so speeding. There were also other states-- Minnesota, Ohio, Kentucky, Massachusetts, Alabama, and Indiana. And those licenses were suspended due to habitual violations, which eventually you got to go, no more police. So she could not get her driver's license renewed.

She was going through some problems, and then she found out that this woman, who is living as her in Michigan, had been married and divorced with her information. She had got into a leasing company for trucks, 18 wheelers, created a fake business with this information. Our lady was getting the tax bill for the business because it's her business. She was getting collection notices. This person had gone to medical facilities and received medical care, some of it mental health-

related medical care, which makes you wonder exactly what's going on-- little clinics, a heart place, radiology.

So it really ran the gamut of what's going on. They found out the perpetrator was a Canadian citizen. They found her and arrested her. She bonded out and then she fled back to Canada, presumably. But the issues were resolved, and we were really excited about that one.

But that's how bad it can get. And going from a case eight months, whatever, to two years, three years, four years, it's very scary how much a person can do when they've just got a fake driver's license, some fake documentation, and then they go from there.

LISA W SCHIFFERLE: Thank you, Ellen. Thanks for sharing those additional faces of ID theft from a victim's perspective. Now we're going to turn to the moderated discussion part of the panel, and I have some questions for the panelists. But I also want to invite everyone here in the audience to ask questions.

So you should have little cards. If you have a question, please write it down on the card and hold it up, and someone will come around and collect them. And we will try to include those questions as well as the questions that I have.

So while we are waiting for the cards, let me ask you all. We talked a lot about the harms of identity theft. I'd like to talk a little bit more about recovery and what are some of the challenges to recovering from identity theft. You want to start, Eva?

EVA VELASQUEZ: Sure. I think the biggest issue we have with our remediation process is how fractured and siloed it is. There are a few types of identity theft where we have a universal process or mechanism in place that works out reasonably well if there aren't too many kinks in the case, but that then becomes very different if it's from financial to medical to criminal-- even to child. Child identity theft versus financial identity theft, the behavior can be the same, but the age of the victim can create an entirely different process.

Because if it's a child, you cannot use the online systems to start checking those records. It all has to be done through the postal mail. So even that small difference creates this process that requires organizations like mine, requires the support of the FTC, to build out these remediation plans that will detail how to handle these things. Because there's so many variables, and the victims don't know how to address those. And they don't know where to go. So if we could do more comprehensive and holistic types of processes, if we could start to integrate them at least a little bit more, I think it would make a world of difference for the victims out there.

ELLEN ABBOTT: I agree with that. One of the examples that we've seen lately-- d employment fraud. So you get a letter in the mail, you get a notice from the IRS that says you've earned wages. I've earned wages. What? That you owe more money because you have these wages earned for the past year at this place you've never heard of.

So you called up the place. The employer may be willing or unwilling to speak about who they've employed and how they've verified that information. A lot of employers don't use the e-

verify system, as they should, especially if it's a low-income factory job. We just need the help. We're not going to go through that process.

So it can impact that from an IRS perspective and then, again, getting the employer to comply and report the information to the IRS-- working with the Social Security Administration, making sure the wage and earning statement isn't wrong with the wrong information. So just kind of the different silos of identity theft where you've got IRS fraud here. You can deal with the IRS, but things like employment fraud and utilities fraud can have a kind of a spider effect where you have to chase down two or three different entities in order to get it resolved.

And don't forget to check your credit report, because it might be on there, too. And you might not be able to get that mortgage that you wanted or that new appliance that you wanted to finance. That's usually how we see a lot of identity theft arise, is someone is trying to get some line of credit or they do want to buy a house.

And the creditor says, sorry, you've got a low credit score, or that judgment on your credit report is really hurting you. What judgment? I don't know what you're talking about. I've got great credit last time I checked. So usually it comes from a financial need of needing something and not being able to get it, because there's things on your credit history you had no idea were there.

LISA W SCHIFFERLE: Tammy, did you have something to add on this?

TAMERA FINE: I think from the people that I work with who are victims, there are two things that really caused a tremendous amount of frustration. The first is all of the secrecy laws that are in place to protect our information in certain situations are sort of turned against the identity theft victim, who's told, you can't get a copy of the tax return that was filed using your identity. You can't see your medical records, because that includes medical records of the person who's stolen your identity and they're protected by HIPAA.

And it's very hard for victims to deal with the fact that the laws are protecting the person who's victimized them and prevents them from doing things like going through their complete medical record and being able to say, that's me, that's not me. It's a very frustrating thing. And then I think the second thing that I see a lot in my line of work is the repollution of or revitalization of the identity theft victim, which happens in two ways.

The first way is when a creditor accepts-- at least says that they accept-- that something's identity theft, says that they'll write it off, but in fact, what they do is they sell it. And then that person goes after you, and then they sell it. And that person goes after you. So that can happen.

And then I have done several cases just in the past couple of years where someone maybe-- we put them in prison for five years-- they come out, and while the ankle monitor is still on, they are out at an auto dealership using their old victim's identities. They've saved this. They've got that information and they use it to jumpstart their reentry into crime when they get out. And so we have the same people having a lull of four or five years and then being victimized again. And we know that the lull was just because the guy that was using their identity was in prison for that period of time.

LISA W SCHIFFERLE: Thanks. And, Amy, I'd love to hear from you a little bit about some of the challenges that you've faced in trying to recover from your identity theft situation.

AMY WANG: Yeah. I love listening to what they had to say, because I don't think honestly I will ever recover. I think it's a disease for our family that will be in remission for a little while. Maybe we're not going to get any kind of information coming in, but all of a sudden the assault is going to happen. We just don't know when.

And what you were saying about the protection-- I have all of this. This is our fraud file right here that I brought just for fun. But this is a letter from the US Postal Service, which is our change of address form, which doesn't say where our address is being changed to. So we have no idea where our mail is going.

Inherently afterwards, we did end up getting the information from mail that trickled through, but we're never going to-- and our children probably aren't going to recover. Because during that time frame, the information that these people got, it really is a windfall. So I agree.

LISA W SCHIFFERLE: Yes, that's a really interesting analogy, the disease idea, that you never really fully recover. You're in remission. Your story actually brings us to one of the questions that the audience asks, which is, why is the post office so slow to respond and can it be expedited? That was one of the things I found so frustrating in listening to your situation, was the challenges you had in trying to resolve the change of address.

AMY WANG: I said, too, you can go into the postal service. I brought this fun prop. And it costs nothing. You can pick this up, your change of address form, although they're trying to sell you a lot of things in here so it's hard to get to the form.

But when you get to the change of address form, it's quick and easy. Drop it in the box, and I could change anybody's address anywhere without any identification. It's a very simple, low-tech way to really impact somebody's life.

EVA VELASQUEZ: You can also pay $1 to do it online.

AMY WANG: And actually online that's how I ended up-- after they changed our address a second time, that's how I had to get my address back. I had to fight fire with fire. Because it was too complicated to actually go through the proper way and go to the post office and call the number and wait on the phone for an hour. And so I got online, paid a dollar.

LISA W SCHIFFERLE: And we heard this morning that 50% of identity theft is not necessarily happening online, so I thought of the post office scenario. I guess it could happen online, like Eva was saying, but it can also happen just in person. So that definitely seems like an area for improvement for identity theft victim services and recovery. I wanted to also ask you how long, in your experience, you think it takes identity theft victims to recover from identity theft.

It varies wildly depending on what's happened to them. So I think, as I said before, if your credit card is skimmed, it's a matter of shutting down the credit card and getting a new one issued. But

if you have the sort of pervasive identity theft that Amy and her family suffered from, it can take years, decades.

EVA VELASQUEZ: Well, it's inconsistent in that even if it's the same type of identity theft and very similar circumstances and experiences, because of the lack of resources-- and I hate to pick on the government here, but I tend to see it more with government identity theft-- because of the lack of resources available to handle the volume of cases that are coming in, it doesn't seem to be that it's first come, first serve. I talk to folks who have reported the issue and started working on resolution at relatively the same time frame, and it is relatively a similar circumstance. And yet one person may have resolution in four months and another person doesn't happen until a year later.

And the only thing I can surmise when I'm looking at that is that because of the impact, because of the tremendous volume, there simply aren't enough bodies and people able to organize and mitigate these cases as they're coming in the door so that they can actually do them sort of in order. Because as you said, it's wildly inconsistent, and I really can't pick a pattern out when we're talking to people in our aftermath study and on our phone lines who are saying, well, but shouldn't this have been done already; I've been waiting eight months; I've been waiting a year. It's like, well, we just have to keep moving forward on it and keep staying persistent.

LISA W SCHIFFERLE: And, Ellen, I think you had some interesting statistics about how long it's taking people you're working with to resolve the ID theft, depending on the type of identity theft? Can you share those?

ELLEN ABBOTT: Our investigators-- from the data we've pulled, a normal average case for all investigators will take around seven to eight months. Now, that's from the ones that are one and done and 45, 60 days, and then you've got the ones that are harder to attack-- like Eva said, any kind of government issue or tax fraud issue or employment issue that each issue involves two or three different entities. Utilities are the same type of thing.

Or if there's a collection account on that file that you close down and then it gets resold-- that's a lot of the challenges we face as restoration investigators, is calling up the collection agency and saying, we've already got this cleared up. We've got a clearance letter. We've had it since 2015.

Do you want us to send it to you? Please don't resell this. This has already been cleared up once. It's really frustrating for the victim, and it's also frustrating for our guys internally.

LISA W SCHIFFERLE: How about you, Amy? How long has it taken you to somewhat recover? You said it's like a disease that you never fully recover from, but have you been able to resolve any of the issues along the way?

AMY WANG: I want to think so, but it took a couple of months-- I mean, a couple months to get our mail back. That was a long-- believe me-- a very long time. But I just don't consider it resolved.

I have this paranoia now that either I'm not going to get the mail one day or I'm going to get another charge for something. I'm just waiting for the next angle. I don't know. I don't consider it resolved in any way.

LISA W SCHIFFERLE: Would the rest of you panelists say that that's a pretty typical sentiment of ID theft victims?

TAMERA FINE: Absolutely.

LISA W SCHIFFERLE: I think that's part of the challenge of identity theft, is it's never fully resolved. You never know when it will reemerge. We have an interesting question from the audience. You all talked a lot about the different types of identity theft and how they pose different challenges, and someone in the audience asked, how can seniors protect themselves from identity theft, especially those who are not technologically savvy?

ELLEN ABBOTT: My first thing I would say, don't answer the phone when people call that you don't know. I know a lot of the senior population may not check caller ID or may just answer and talk to whoever's on the phone. I'm using my mom as an example. She's a very nice lady, very southern woman in Nashville, Tennessee. And she'll pick up the phone and she'll talk to whoever's talking to her.

And she got the call from the scammers, that we'll fix your computer for $200 and all this. And she's like, let me have you talk to my daughter, because she knows all about that. So they called me, and they didn't care where I was. I'm like, I'm not at my mom's house; do I need to be?

So I kind of played a little game, and it was funny. Because we know they're scammers, and it's like, let's keep them on the phone, waste their time. They're wasting our victims' time. So yeah, it's like don't answer the phone, don't give them any information.

A lot of it's fear-based as well. So if they have a stern-sounding person on the other line saying, we're going to put you in jail because you didn't pay the government or you didn't pay your taxes-- well, I know I paid. Well, let me go ahead and write you a check.

It's like, no, please, don't do that. You don't know who this person is. Don't give them your social security. Don't give them your checking and routing number.

Or a lot of the scams where, my granddaughter said she was stuck in London and she needs money to get back. And it's those scams where they fall prey to sending wiring money, and then they're also a little complicit in the fraud, where the bank is not going to be very willing to listen to the story of I got tricked into doing it. Well, you're out that money now. We're not going to reimburse you on that.

So I think for the older population it's just don't entertain conversations with people you don't know, especially when they're asking for some kind of money, some kind of thing in return, some sort of access to your computer or your information, your checkbook. Just be really leery of that. And I hate to put that fear out there, but it's the kind of world we live in now.

LISA W SCHIFFERLE: That's exactly in line with the advice the FTC gives, too, in our Pass it On campaign, which is an anti-scam campaign aimed at older adults. And it basically says, just hang up and don't give out that personal information or give money over the phone, especially if someone else called you. You don't know who it is.

TAMERA FINE: I speak a lot to elder groups, and one of the things I tell them is to sort of practice ahead of time. Know what your rules are. Know that you never give out information over the phone. You never give anyone your PII over the phone.

Know that you never commit to buying something over the phone. If someone comes to your house to sell you something, you tell them you'll go speak to another provider, but you don't give money or a job to someone who comes up to your house. There would have to be just bright line rules, and you have to practice saying no.

Because particularly for a lot of elderly people who sort of matured before the current era, they have a different view. They're very polite and they want to be helpful and they want to be accommodating. And you really can't be, because if you are, you're going to be taken advantage of.

LISA W SCHIFFERLE: Great. And one of the other issues I wanted to touch on is something that Eva raised in her remarks, which are about the ripple effects of identity theft or the downstream effects or lost opportunity cost from identity theft. In other words, how might the community as a whole pay the cost for identity theft?

EVA VELASQUEZ: Would you like me to comment further on that?

LISA W SCHIFFERLE: Go ahead. That would be great.

EVA VELASQUEZ: Again, the lost opportunity costs and I think how they travel down into our communities-- I usually tell stories about that. And they can be very-- I guess subtle would be the word. And I think, because I covered some of this-- you know, Amy talks about an experience that she had after she thought that her case-- I think you said your case was over. And I actually think this will be a better illustration, because I've already kind of talked about some of what we see through the aftermath. So, Amy, would you share that?

AMY WANG: I have some rental units, and I was doing some rehab on one of these units. And I had to hire workers for a few days to do some work. And I have to turn the electricity on, turn the electricity off. And so now that I had an alert with the credit bureaus, I have to pass my own identity test, which is actually quite difficult.

So I failed the test a number of times, because now there is all this erroneous information connected with us and our family. And so if I can't pass those tests, I can't get the electricity turned on. If I can't get the electricity turned on and it's 95 degrees in Miami and I need power tools plugged in, guess what?

Everybody has to go home for the day, and these guys that I tried to hire are guys that make a lot of money. So a couple of days that go by and they don't get paid, that's a lot of money to them and their family. And for me, it's a few days that I don't have rented, and it goes on and on in time. So yeah, there is definitely an extension of the effect.

LISA W SCHIFFERLE: That's a great example. Tammy, when we talked before, you mentioned an example from one of your cases involving a security clearance and lost job opportunities?

TAMERA FINE: I had a really heartbreaking case. We don't typically do what we call single purpose, single victim cases. We typically are looking for gangs. But we had a young woman who was clerking for one of our district court judges and had her identity stolen and all sorts of credit accounts opened in her name and the like. She had put herself through law school at night, working during the day and law school at night.

She was now a district court judge's clerk, and she was offered a position in the honors program, which means you don't have to go work for a law firm. You go straight to the Department of Justice. It's a great program. She was clearly a wonderful candidate.

She couldn't pass the background check because of all of the things that were going on with regard to her credit history. She thought she would get it cleared up, and then something would pop up and she would lose it again. This is what she wanted to do. She wanted to work for the Department of Justice, but she had to be unemployed for six months. Because if you take a different job, you lose the offer from the Department, and yet she couldn't start with the department because she hadn't passed the background check.

So you can imagine for someone of her background the loss of six months of salary, the harm to her family in terms of them having to support her for that period of time, and just the emotional turmoil that she felt. Because she had done everything right and achieved this wonderful position with the Department of Justice, and it was being stolen from her over and over again by someone who was using her identity.

LISA W SCHIFFERLE: Thank you for those stories. We have another question from the audience, and this one deals with the topic of selling debt that's run up through cleared identity fraud. I guess they're talking about the issue when there's a debt and someone has said this debt was due to ID theft, and yet someone sells that debt. And this person is asking, isn't that fraud? Do you have anything to say on that?

TAMERA FINE: I guess as the prosecutor, I should be the one to answer that question.

LISA W SCHIFFERLE: I think they may mean fraud loosely rather than--

TAMERA FINE: You're exactly right. It may be fraud loosely. It depends on what's told. We don't know what the discussion between the individual who sells the debt and the individual who buys the debt is. They typically wildly discount it, though, so they're paying, like, $0.07 on the dollar for the debt. And they know that they're getting debt that is compromised and maybe uncollectible, and they're willing to buy it anyway.

So my guess is that it would be very hard to make a fraud case out on that in terms of the two people engaged or the two entities engaged in that transaction. The more interesting and difficult question is, is that fraud with regard to the individual whose identity is at stake in terms of the underlying debt? And that would be a case I would be interested in looking at, because it would be a way of trying to stop those downstream harms.

LISA W SCHIFFERLE: We're getting a lot of good questions from the audience, so I want to get to another one, which is how much of this identity theft is by people who know you, like familial identity theft or friends?

EVA VELASQUEZ: Oh, I wish we had good statistics on that, but we don't. And the reason that we don't is because often people don't really know where their information was compromised. They have a guess. They think it was so-and-so, and of course it's not until there's actual investigation and prosecution or an admission of guilt that they can confirm that.

And it also goes, I believe, drastically under-reported. Because when we talk to people who are dealing with either a parent or a family member and the decision they have to make is, I either need to report this family member to law enforcement so that I cannot be held liable for something that I didn't do or I have to stop having a relationship with my family, period. And I have personally talked to victims who have had-- it's like the Hatfields and the McCoys, and they have family dynamics where one side of the family is going, if you don't report mom and dad for doing this to you, I'll never speak to you again.

And the other side is going, if you do report them, I'll never speak to you again. So I do think there's a lot of under-reporting, and because we have so few prosecutions I think there's a lack of confirmation that is allowing us to get good statistics in this area. But from an anecdotal perspective, when talking with people on the phones-- we talk to about 11,000 individuals on an annual basis, so we have a pretty good sample of stories and experiences. It's a crime of opportunity, so it's people that either are related to, live in the home, caregivers. It's that type of dynamic.

LISA W SCHIFFERLE: Thanks, and we have a couple more questions from the audience that I want to get to and then I have a closing question. The next question from the audience is, how effective is a credit freeze or a security freeze in preventing identity theft? And could credit bureaus do a better job in helping to prevent identity theft, or is the onus on service providers who open new accounts without authenticating the new customer? Anyone want to take that?

ELLEN ABBOTT: So I can speak to the credit freeze and the fraud alert piece. If you need a credit freeze, it's good, but it's not a silver bullet. So when people rely on a credit freeze to totally freeze their credit, they have to put a pin number. There is some management involved. If you're not a confirmed victim, there may be a cost, depending on your state.

So there's good things about it. Most of the time it should shut it down, but if you've got a relationship already established with one of your creditors and the thief knows that and goes on to open a new Capital One credit card or whatever it is, they'll say, OK, because they already have access to the credit. It's not frozen for existing creditors.

They have that access to it. So that's why we tell people if you really need a credit freeze, understand there's management and understand that it's not a silver bullet. There's a second part to that question about--

LISA W SCHIFFERLE: The second part was whether credit bureaus could do more to prevent identity theft or whether the onus is on service providers.

ELLEN ABBOTT: I think it's both. I think service providers, there's a lot of easy credit to get at retail stores. Here, you want to open a new credit card today for 15% off? Sure. And the point of sale teller may not follow the rules that are supposed to be set up from corporate, or there may not be enough training from corporate. Or it's not consistent.

The credit bureaus also-- there's room for improvement there, especially from a seven year alert perspective. We have a case that one of our investigators is working where they had issues. The husband had issues. He had a seven year fraud alert on there.

The thief was able to call up the credit bureaus and take it off just by phone call. And they knew enough information that they answered the questions correctly. So that seven year alert came off. As soon as it was off, thieves went in, went into a retail store, bought $15,000 worth of products, and they were out the door.

Now, we've got him on camera, but nobody's willing to prosecute. So that's the frustration of seven year alerts and credit freezes and then the challenges there about better training and better education for credit bureaus and creditors alike.

TAMERA FINE: You also have the problem that credit alerts really only cover certain portions, certain types of identity theft. So if someone's getting a driver's license in your name, that's not going to hit your credit report. The credit freeze is not going to stop that. So when you look at sort of the entire universe of what can be done with your identity, a credit freeze really covers only a small percentage of it.

LISA W SCHIFFERLE: Thanks. And we do have one more question from the audience, which I'm actually going to defer to the next panel, because it's asking about how much identitytheft.gov has helped the victims' community. And I know we're going to have a whole presentation on identitytheft.gov from Nat Wood, the Head of the Division of Consumer and Business Education.

So you'll hear about that more in the next panel, but I do want to close this panel by asking each of you, if you could wave a magic wand and change one thing for identity theft victims, what would that be? And we can just go down the line here.

AMY WANG: I want a genie in a bottle. I want three. I would like to see this get some streamline, innovation, and education. And I think those three things-- in education, I mean, from the ground level up, I like the IRS's campaign and how they've taught people, don't give anybody information over the phone but educate people in terms of the community-- bank tellers, store clerks, postal carriers, everybody, across the board, police officers.

LISA W SCHIFFERLE: And, Tammy, what would you do with your magic wand?

TAMERA FINE: I think I would have the world exist where a credit reporting bureau, when they get a new application for credit for someone that doesn't have a record, can actually verify with the Social Security Administration that that name goes with that social security number, that that's a real person. Because that would really shut down child identity theft in a big way.

EVA VELASQUEZ: That would be exactly what I would say.

LISA W SCHIFFERLE: Ha, ha, ha. Ellen?

EVA VELASQUEZ: That is exactly what I was going to say. Right now, the social security number should not have the level of importance or weight that we give them. We heard in an earlier panel that they are a tool that is being used for something it wasn't designed to be used for. And so in that perfect world, we should no longer use that as the primary identifier.

However, we don't live in a perfect world, and in the meantime, while we are trying to achieve that goal, we need to put some things in place that allow for more verification of that number directly with the source. Because it's anemic right now. It's possible, but it's anemic and it's not being done.

And it would. It would basically eradicate child identity theft if we could just get-- does this date of birth match the social security number? No? Done.

LISA W SCHIFFERLE: Thanks. And, Ellen, what would you change for identity theft victims?

ELLEN ABBOTT: I would want better enforcement of the FCRA laws, the FDCPA, the laws that govern disputes for fraudulent accounts. So if a person sends in their information like they're supposed to, they follow the guidelines, it shouldn't take 90 days. It should take 30 days, like it says in the law. So enforcing those laws.

They're suitable as they are. They just need a little bit more meat to them, maybe bumping up some fines for those who violate those laws and the collection agencies who resell the debt and things like that. So it's something that it's already there. We just need to enforce it better and make the creditors and make the credit bureaus really have to follow those rules.

LISA W SCHIFFERLE: Thank you all for sharing your experiences and expertise about the victim's perspective on identity theft.

[APPLAUSE]

RYAN MEHM: Good afternoon. My name is Ryan Mehm. I work in the FTC's Division of Privacy and Identity Protection, and I will be serving as the moderator for this panel. I'd like to thank all of you who stuck it out today, as well as those who are still watching on the webcast. Thank you so much. While the panel immediately before this considered the impact of identity

theft on victims, this panel will address resources and tools available to consumers that are identity theft victims.

We are extremely fortunate to have with us today three people with deep experience on these issues. To my immediate left is Nat Wood, Associate Director of the FTC's Division of Consumer and Business Education. To Nat's left is Laura Ivkovich, and Laura is a Policy Analyst at the Office for Victims of Crime at the US Department of Justice. And to Laura's left is Eugenia Buggs, a Vice President at Generali Global Assistance.

Each panelist will be giving a short presentation and, like the last panel, following their presentations, we will have a moderated discussion. There were a lot of questions submitted by the audience during the last panel, which was fantastic, so I encourage you, keep them coming.

We have cards that are available outside. I think they're available here in the room. If you have a question, write it down, hold your hand up. Someone will come around and deliver it to me up front here. So with that, I will turn things over to Nat.

NAT WOOD: Thanks, Ryan, and thank you all for being here. It's really great to see that so many people have been here today representing so many organizations that have an important role in the identity theft prevention and recovery space. One of the themes we've heard throughout the day is the importance of partnerships. Eva in the last session said, there's still a lot of silos, and that's definitely true.

And the way to break that down and help people have a better experience is by working in partnerships across our different organizations in government and out. Most of what I'm going to talk about in this presentation is identitytheft.gov, which we hope is a great resource for all of you, as it's been a good resource for more than 500,000 identity theft victims since we unveiled this new system in January of 2016. The idea behind identitytheft.gov was to go beyond just providing people with general advice and to leverage the information in the reports that people give us about what's happened in their identity theft experiences so that we can create a personal recovery plan for each of those victims.

In addition to getting a personal recovery plan, which we'll walk people through step by step what they need to do, we provide an FTC identity theft report. And I'm going to explain a little bit more about what that is. And we're working very closely now with the IRS, so that we'll be able to transmit the IRS identity theft affidavit directly to them, which is another example of sort of breaking down these barriers.

So on the screen is identitytheft.gov. I'm going to walk through a little bit of what the victim experience is on the site. So once you click, Get Started, you get set down a path based on what's happened to you. We're going to follow the I Want to Report Identity Theft path. I'm going to go through these screens pretty quickly, but this will give you a general idea of what people will experience on the site.

So in this situation, someone is going to report that their credit card has been misused. There are lots of different options, and there are options for combining different experiences, so that if

you've had a credit card opened up in your name and also utility fraud, we'll respond to both of those issues. When you go through the system, you're going to get the identity theft report as well as your personal recovery plan. I'm not going to go through what every screen is like, but this is the FTC identity theft report.

And this is a key feature of the identitytheft.gov system, because this is an official report to law enforcement under the Fair Credit Reporting Act. So you should be able to take this to the financial services industry, to credit reporting agencies, and trigger your rights under FCRA by delivering this FTC identity theft report. We're working closely with law enforcement, the financial services industry, and the CRAs to make sure that that's actually the experience that people are having, and we're making a lot of progress. We're not 100% of the way there, and that's why I hope that we're getting that message out through this event.

After you submit your report, you get your recovery plan, and it's very specific to what you have reported to us. So in this case, it's not just going to say call your bank. It's going to say, call Bank of America, because that's what you've told us is where you're having a problem, and give you other steps along the way.

Once you get into the plan, you can check off step by step what's happened. The plan will adapt and change over time as you take the steps that it lays out, so that if you send a letter to a company the letter is going to be generated by the system. But if that doesn't solve your problem, we're going to tell you what the next step is. So it's a very robust system.

Here's an example of one of the letters. So if you are in the financial services industry or in debt collection industry or working with credit reporting agencies, you may be seeing these letters, and that's a good thing. It's a good thing that we're helping people with the letters. And as I said, if you are following these steps and you hit a roadblock-- in this case, you found something on one of your credit reports that is wrong-- we're going to walk you through the next steps.

And I'm going to have an opportunity to talk a little bit more later, I think, about the resources. But I do want to remind you, because I'm not going to spend a lot of time on it now, that the FTC also has print publications. For those of you that are here in the room, there were some of those outside in the hall. And if you go to ftc.gov/bulkorder, you can order those in bulk to share in your community. So if you are with an organization that helps victims recover from identity theft, you can get free resources to help you do that from ftc.gov/bulkorder.

We've talked a little bit in some of these panels about the intersection between different frauds and scams that lead to people's information being compromised and their identities being stolen. A great way to learn about what the latest frauds and scams are and how to avoid them is to sign up for scam alerts from the FTC. So you can do that by going to ftc.gov/scams. So with that, thank you very much. I'll hand it off to Laura.

LAURA IVKOVICH: Great. Thanks so much, Nat. Nat gave us a great overview of what the FTC is doing, and now Laura's going to speak about what DOJ is up to. And like my colleague from DOJ mentioned, I'm here as myself and not representing the policies of the Justice

Department. But I have been working in this area for quite a while and have lots of federal partners with me today and in solidarity on our fight for victims of identity theft.

So I'm going to tell you a little bit about a small but mighty office that I work for. Many people don't know about it, and it's in the Justice Department. We're a non-litigating office, but my presentation is going to walk you through a little bit about what I do at the office, how we get our funds, the services that are available for victims of crime. The small secret is it comes not from tax dollars. It comes from convicted federal offenders.

So those fines and penalties go into a fund that our office handles. The benefits go back to victims of crime, so it's kind of a cool restorative justice model-- a new grant opportunity that's going to be hitting your town soon, so that you should be one of the people to either sign up for it or be a brochure to your colleagues to help maybe have them apply to be a coalition that helps victims of identity theft.

And then some of the benefits of collaboration. Basically, you're force multiplying when you collaborate on these very, very complex cases. In many instances, they're just so complex you need more than one person's help to get through them.

So the Office of Victims of Crime in the Justice Department didn't just come out of nowhere. It came from a president's task force report in 1982. President Reagan established it. And it was to help basically have the systems do a better job of working with victims who were often called upon as witnesses, and we were not really looking at the needs that they were suffering from from the crime itself.

So the task force was charged with putting some recommendations out. And some of the things that came from that was the establishment of our office, so that was a very good thing-- and the establishment of the fund. So those are 30 years ago pretty much, and we've been working since then to get money out to states in formula grants. So every state in the nation and territories receive funding to set up victims' services through formula grants that our office handles.

And then also there's state compensation programs. Those are a little different. I won't go into a lot about that. And then there's discretionary programs at our office overseas, and these are where most of the programs that I've been involved in my last 25 years working for the Justice Department have stemmed from, these discretionary grant programs.

So this is just a chart to show you that we have three pots of funding, and the blue colored version is the victim assistance. And that, as I mentioned, goes to the states, and that's really to provide direct victim services. Our money generally goes for things like domestic violence shelters, sexual assault programs, child abuse programs, prosecutor-based victim services, other community-based services, anything that can help a victim get through the process of having been victimized, and, especially if they're within the Justice Department, working with the criminal justice agents who need their help and cooperation in bringing a case to prevent the next victim from being harmed by that bad actor's acts.

So annually, we put a lot of funds out on the streets. And this is where our money comes from-- as I mentioned, convicted federal offenders. In the past, in fiscal '14, we've been doing a lot with a little. We're only 30 people in our office, I want to say. We're a very small, but mighty office.

And fiscal year, our cap on our funding has been in the $745 million range. We had a windfall in fiscal '15, and thanks to Tammy Fine and her colleagues who apply those criminal penalties against the fraudsters, that money keeps growing. And there's billions in that fund.

So we were able to, and Congress was so wonderful in allowing us, to have a cap raised. So now our funding is at $2.36 billion in '15 and then $3.4 billion or so in 2016. So we had a huge increase. So the field-- when I say the field, I mean the states that decide where the funding goes-- are now making these really big decisions on where this funding is going to flow to. And identity theft victims' programs is where they ought to also be putting priority and emphasis, since the numbers are so large on these kinds of cases.

So the money, as I said, is a lot. It's going back out to the states. That's the lion's share of the money goes back out to them. We also work in our office to do things like put up online where that money goes, and the Online Directory of Victim Services is one of those places where you can search by zip code, by type of crime, by location, by service provider, by identity theft, and find the programs that are being funded at the local level through our federal dollars.

Again, there's a lot of them and it's a good resource for you all to look for in your locales. The other thing I mentioned is that our office, through our discretionary side of the house, funds national scope training and technical assistance programs. So one of those programs that I've had the honor to be the grant monitor of is the National Identity Theft Victim Assistance Network.

It's a coalition-- a network of coalitions, I should say-- that bring together individuals much like you in the room and victim service providers who want to do a better job of being able to help the Amys of this world recover. And thank you, Amy. I meant to say that earlier for your story, and we really appreciate that.

So this network has been doing really wonderful efforts, and we've funded 10. They all have different areas that they've focused on-- some domestic violence, some low income, and other types of cases. But from their work, we've amassed a lot of materials that are available online that others can access, including tip sheets and ready-to-use forms and things like that.

We are now announcing a new funding opportunity, and the resources that Nat just said were out on the table included one of these pamphlets is basically the information about that program. And we are making 20 new coalitions available with funding. It's a three year project and we're making $50,000 available as sub-awards to each of the programs. And the Identity Theft Resource Center is the overseeing grant agency that's going to be working on that.

I know I'm out of time, but we also have online resources available. And this is to help new people learn how to work with victims of crime it's intended for victim advocates, but it could also help others, maybe customer service representatives or, if you run hotlines, maybe people

who are going to work on the hotlines, incoming interns who might be working just for a little while, maybe the summer or whatnot, on some of your cases. This might be a very helpful tool.

And lastly, we have a mobile app that our office has funded through the Identity Theft Resource Center as a helpful tool. People aren't always using the computers at home. They're mobile and they're ready, and they need help immediately. And this is one of the things that we've tried to do in a technologically savvy world, is try to keep pace with that.

Our 1-800 numbers and our call centers are now doing chats and texts. It's not necessarily a pick up the phone and talk to victims by that old method. So we're trying to stay current, and this is one of the tools that we've tried to stay current with. So I'm passing the tool to you.

RYAN MEHM: Thanks, Laura. And next stop is Eugenia Buggs, who will give us the perspective from the private identity theft service providers and what they're doing to help victims of ID theft.

EUGENIA BUGGS: Sure. Thank you. As Ryan said, my name is Eugenia Buggs, and I'm the Vice President of Global Marketing for the Identity and Digital Protection Services unit of Generali Global Assistance-- quite a mouthful there. It's my pleasure to be here today. But I want to make sure that we stay on track, so I'm going to dive right in. I think even if you didn't know it, if you've been here all day today, one thing that has become a reality this afternoon is that risk is a reality.

So I want to start by saying that there is no company or service that can guarantee that your identity will never be stolen. It's unfortunate, but it's true. So if you have a provider or organization that's telling you that, run the other way because it's simply not true. It's not much different from having a home security system and that not being able to guarantee that no one will ever break into your home or having a car alarm and that not being able to guarantee that no one will ever break into your car or steal it altogether, for that matter.

There is no such thing as perfect security, but that doesn't mean that you should just kind of stick your head in the sand and say, well, forget it, if there's nothing I can do about it, I'm going to become a victim at some point anyway; I'll just wait for the inevitable to happen. And that's because there's a lot at stake. I think that, again, if you've been here throughout the day, just the panel right before us, hearing Amy's story, you understand that there is really a lot at stake. We've heard a lot.

Typically, when people think about identity theft, they only consider the financial loss part of it. And as the panel mentioned earlier, you think about your bank account being drained, someone running up credit card bills in your name or something like that, but there are a lot of other aspects to it that the panel before me put very eloquently. So I won't rehash a ton of them, but we've talked a lot about medical identity theft. And so in that one in particular, there's the financial aspect in the sense that you may get a bill from your medical provider from your insurance company when somebody has used your name to get medical services.

But the other side of that is you now have this information commingled with yours. Maybe this person has a different blood type than you. They may have a different set of allergies. And again, as was mentioned earlier, if you're in a medical emergency situation and you can't verify that this information is inaccurate, that could really have dire consequences.

So next, I'm going to kind of dive into some of the services that are typically available through the identity protection providers. I'm going to go a little bit out of order here, and I'm going to start with monitoring and alerts. And that is because most of the time when people think of the services like we provide, the first thing they think of is the credit monitoring. So that's going to monitor for changes to your credit score and your credit profile with one or all three of the major credit bureaus.

But there's another piece, and that is the identity monitoring. Identity monitoring is going to monitor for all of those non-credit things. So that could be anything from someone getting a payday loan in your name to your social security number being bought and sold in bulk on the deep web in some of the sites that we heard in some of the panels earlier as it relates to larger data breaches or things like that.

The other thing I want to mention here, too, is that as it relates more specifically on the identity monitoring side, it's going to be very difficult for the average consumer to ascertain why the identity monitoring for service provider A is X times better or worse than the identity monitoring for service provider B. And that's because of a lot of the way that the identity minoring works is using proprietary software, is using complicated algorithms. So even if a person can actually get the information from the provider, it's going to be complicated for the average person to actually understand it, and it often changes.

Because as the criminals get smarter and change the way they do things, the monitoring also changes. I think the important thing for consumers to note here is that if you have a service like this, it should include monitoring and you should be monitoring both the credit and the identity. Some of the things that I'll move into next that are a little more easy for the average consumer to kind of get at what I call key considerations that consumers can quickly or much easier be able to figure out are some of the buckets I'll go through here.

First is prevention and education. Prevention, depending on the provider, can manifest itself in different ways. Often it's some sort of online data protection, which is going to be software you can put on your computer that's going to keep you from going to phishing websites or something like that.

But more importantly-- I'm really glad Amy spoke about this earlier-- but it's education. If you have a service like this, you should be getting information on a fairly regular basis from that provider about trends that they're seeing, what sort of fraud scams are going on out there. They should be giving you tips to reduce or mitigate your risk. And then the last thing I'll jump to is support in that section.

Another thing is if you have a provider, you should not only be able to call their customer service, or what we've referred to as the solution center, after you've become a victim of identity

theft. You should be able to contact them and say, I got this really weird letter, what should I do about this, I don't know, or I got this strange phone call, and really get assistance in advance of becoming a victim. The next thing I'll move into is the resolution.

One of the things you want to make sure is that it's full service. I mean, resolution can run the gamut from you contact them and they give you another set of phone numbers to call and really kind of have to figure out how to resolve it yourself, all the way up until what we call full service where you explain the situation and give the provider the authorization to resolve the situation on your behalf so that you can really focus on living your life.

The other thing is that it should be available 24/7. You want to make sure that they're not only available nine to five, Monday through Friday, because that's oftentimes when you need to be at work and focused on your own life. And outside of that, if you're traveling, we know that people have a higher risk of identity theft when they're traveling. So if you're in another country and your wallet or your purse is stolen, you don't want to have to be worried about time zones and can I reach them. You want them to be available to help and assist you 24/7, 365.

The last piece is insurance. A lot of providers now have some sort of insurance or what people think is insurance in the services that they're providing. So you want to make sure that number one is an insurance and then if it is what's actually covered. If you need to get an attorney to handle some sort of litigation related to the fraud situation, will that be covered up front or will you be reimbursed? All of these things.

The point of it all is that these services are not all created equal. I know at this point people feel like I've given them so much stuff to go and research and now I have another homework assignment and I already have 50 million other things I need to do every day. So when I hear that from consumers, I often tell them they should start with organizations that they already know and trust and have relationships with.

So reaching out to their financial institutions, their insurance companies, their employers offering a service like this as an employee benefit, or some sort of affinity organization that they're already a member of to offer something like this is a benefit. Push that back on those organizations that you do business with already and let them do the due diligence to find providers that will offer comprehensive services that you're really getting what you think you're getting when you sign up to pay for it. And then beyond that, the level of service that you're going to receive if you ever do need to pick up the phone and talk to somebody on the other end is going to be comparable to what you've come to know and expect from the provider or the institution that you're getting the service from to begin with.

So I've gone a little over my time, and I could talk on and on and on about this. But I'll open it up for their questions, because I think that's going to be the more interesting part.

RYAN MEHM: Great. Thanks, Eugena. We're going to start now the moderated discussion portion of the panel. We got a lot of great questions from the audience. Hopefully we'll get to all of them. We'll try to get from them as quickly as we can in the time we have remaining.

I want to start with a question for Laura. And we, Laura, heard today from several panelists, including Sean McCleskey earlier today, Danny Rogers, and others about how ID theft is increasingly tied to other crimes like domestic violence and human trafficking. So I have a two-part question for you, which is, one, what are some of the special concerns associated with these crime victims and what services are available to them?

LAURA IVKOVICH: Thank you for that question. I will say that what maybe runs through a lot of that is the complexity of detangling what is already a complex crime. Domestic violence and human trafficking have very many different elements associated with them. One piece of that is the use of someone's identity to hang over them or the threat of ruining their name and their credit so that they can't escape or they can't get away, or if they try they're not going to be able to survive or make it in this world because it's been ruined. Or I'm going to ruin you, or I'm going to turn you in.

So there's a lot of similarity in those kinds of victims' lives, that they are either under the thumb of somebody who is using their identities as a way to keep them enslaved in any dangerous situation and the complexity of repairing when somebody does perhaps leave or escape or get out of that kind of abusive situation, the changing back to a more normal state of financial health for that individual's identity and that individual. Thankfully, since we fund so many domestic violence programs around the nation and we have so many great attorneys who have been funded by our office to provide legal assistance-- many of them need the legal assistance to get through that-- they're able to avail themselves of those services.

That's what victims' services often do. They help somebody become whole-- not just one piece of it, but the whole ball of problems that victims present when they come to a victim service provider. And oftentimes it is a legal assistance that they might need, a civil legal assistance to detangle or to help them through that process.

RYAN MEHM: Great. Thanks. I've got a question here from the audience for Nat, and it deals with identitytheft.gov, and the question is, why should a victim bother reporting through identitytheft.gov instead of contacting directly the credit agencies or the credit reporting bureaus, for example, or credit card companies or whoever they might have their issue with? Why start with the FTC's resource? Why not go directly there?

NAT WOOD: There's a couple of good reasons why identitytheft.gov should be the first place for most victims to go. One is that all of those reports about identity theft are then made available to law enforcement across the country through the Consumer Sentinel Network. And so US attorneys' offices, state attorneys general, local district attorneys that are members of the Consumer Sentinel System can use that information in their investigations and build what can be very complex case files.

Also, because you never know what's going to happen over time, if you are experiencing a type of identity theft where are you you're going to have more than one step, this will give you an opportunity to follow up. So if you're an identity theft expert and there's just charges on your credit card, you might just go ahead and take care of that. But if you see a second thing happening, it's sort of good to build a record of that, and your personal recovery plan that you get

from identitytheft.gov is a good way to keep track of all that information if you're not an identity theft expert to show you what you should do in all of those eventualities.

RYAN MEHM: Great. Thank you. I have a question for Eugenia which dovetails directly with a question from an audience member as well. So to what extent are identity theft service providers attempting to incorporate medical ID theft in their service offerings and what are some of the obstacles to doing so, assuming some are attempting to do it?

EUGENIA BUGGS: Yeah, I would assume that most are attempting to do it. We certainly are. I think that some of the obstacles that are in place right now is that while so many medical companies and medical providers have moved to electronic records, they're not all housed in a central repository or database so to speak at this point. And I'm not advocating that they should be either, by the way, because that could have some unintended consequences.

But each major company-- take Aetna, for example, United Healthcare, for example-- they've invested a lot of money I'm assuming in technology to be able to have electronic records, and those systems don't necessarily speak to one another at this point. And so it becomes more difficult for a monitoring company to be able to monitor all of the different health care databases that are out there, versus if they were able to communicate with one another, there would be an easier way to kind of get after that.

I know that there's a lot of hard work being done by our company and I assume other companies in this space to really get out in front of that, but a lot of it is going to also rely on the health care providers, for them to get together to allow those databases to speak to one another. I think another thing that's important to note here is that for a very long time medical providers were more concerned about-- I think someone else mentioned this earlier, too, about-- the fraud that they were more concerned with were providers overbilling or putting in additional building codes. They weren't necessarily looking at the fraud from the victim's standpoint of medical identity theft, from that perspective. And I think now that that has become more prevalent, they're looking at how do we address that piece of it, whereas their focus had really been on another type of fraud prior to recent history.

RYAN MEHM: I have a question here for Nat, and it's another audience question, which is, can a criminal go to identitytheft.gov and attempt to use the system to distort my identity?

NAT WOOD: I think if you sort of think about it as a spy versus spy type of-- you know, what could a really motivated kind of criminal do to mess with you-- yes. But I'm not sure what the upside would be. So it's sort of like vandalism. You could put bad information into the database, but you still have to go through the process of dealing with creditors, dealing with the credit reporting agencies.

We're not dumping data directly into those. In fact, like I said, we're working on transferring some information directly to the IRS, and we've thought about this issue. The content of the FTC identity theft report are not verified, but they're also not verified now or in the past in places where people would be reporting.

So some of the remediation steps may require extensive contact with a credit reporting agency or with a creditor. We do sort of at the end of the line. If you work through the personal recovery plan and you're still having problems, we send people to the Identity Theft Resource Center to get more personalized assistance, and sometimes that that's required.

So we're not presenting identitytheft.gov as a cure-all that you're going to go on and you're going to enter some information and immediately your problems are going to be solved. Unfortunately, it's a complicated system. However, for people that are experiencing the angst of what do I do, we're going to walk them through the steps of what they should do and give them as many tools, letters-- and the FTC identity theft reports are among those-- to make it easy for them.

RYAN MEHM: Great. I want to talk for a moment about the dark web. We heard a lot about that earlier today, particularly this morning. And the question is for Eugenia. And we understand, and you mentioned this in your presentation, that many service providers provide an alert to consumers once the service provider spots the consumer's info on the dark web. So I have a three part question.

Part one is, what generally are you guys monitoring when you talk about monitoring the dark web? Two, why is the alert helpful to a consumer? And number three, probably the most important part question, is, once the consumer gets this alert, which I'm sure is very alarming-- we found your info on the dark web-- what is the consumer supposed to do?

EUGENIA BUGGS: I'll try to remember all three parts of that. So the first part of the question related to--

RYAN MEHM: What are you guys monitoring?

EUGENIA BUGGS: What are we monitoring. So in general, as I mentioned, what's being monitored related to identity monitoring is going to be all the non-credit things. And specifically for our service, a consumer or customer can put into our dashboard any number of pieces of information that they would like to have monitored.

So a lot of it is related to how much information they're willing to put in for us to monitor. So it can be anything from your passport number to your medical ID number that's on your insurance card, for example.

What's another good example? Your rewards numbers for your card. So it really can be anything that you prefer to have monitored. A lot of it is about how much trust the consumer is ready to put into the system to watch things be monitored. And I think over time, as people start to see the alerts, they're like, wow, you really are finding things, and they feel more comfortable adding more information in to be monitored.

When you talk about how the monitoring is working or where it's happening, again, a lot of it is proprietary software's algorithms. But in general, I think things to consider are a lot of it is bots, so it's machines that are harvesting data on a larger scale on the dark web. And if consumers are looking for a way to determine one monitoring versus another, keeping a look out for is that

there's also some sort of human intelligence or human operatives out there that are also doing some of that monitoring, too. Because as good as computers are, there are still things that humans are better at.

So our monitoring allows human intelligence that can follow these threat actors. We saw earlier today one of these sites on the dark web. They have a Twitter account. It's crazy. So our human intelligence folks are monitoring them on social media to find out what networks they're going into, which allows us to be able to get at some of this information more quickly and know where they're going next, to know there is a data dump coming or credentials are about to be sold on this particular website, so that we can be looking out for that and monitor consumers sooner rather than later.

Once the consumer does receive that alert, the first thing that we recommend is that they call us, they contact us. Because depending on what they are alerted to and what pieces of information are found, we'll assist them in a different way. If it's their social security number that's found, for example, we may help them with getting a fraud alert placed so that that Social Security number can't be used to open up fraudulent accounts in their name from there. So I think it really is going to depend on that. If it's the medical ID number, for example, that's found, we would want to get them in touch with the insurance company, make sure that they're looking at all of their medical records.

The good thing about the fraud alerts that people are going to receive-- it's not necessarily an alert to say that fraud has already taken place and this is where the preventative piece comes in. It is an alert to say it's out there. Now here are things that you can do to try to minimize the chances of you actually becoming a victim of fraud. So if it's something we call compromised credentials-- so your email, usernames, and passwords, for example-- we talk all day about how often we're all victims of reusing that same information over and over again.

So that can alert you to say, I need to go in and change all of my passwords and usernames and get out in front of the fraud. So in a lot of cases, as I said before, there's no silver bullet, there's no perfect security, but the identity monitoring is one piece that can really help you get out in front of the fraud. So you get the alert. The first thing we recommend that people do is contact us so we can walk them through what needs to happen next.

RYAN MEHM: Great. Thank you.

EUGENIA BUGGS: Did I answer all three parts?

RYAN MEHM: You did. So my next question relates to medical identity theft. We've heard a lot about it today. There's a huge amount of interest in that issue. And again, this is an audience question that I got a couple of minutes ago, and I'll open this up to any panelist who wants to take it. And it's, what resources or methods are most effective to help victims recover from medical identity theft?

EUGENIA BUGGS: Before we answer that, one thing I want to jump in and say-- and I don't know if it was mentioned earlier, but I don't think I recall hearing it as it relates to medical

identity theft. I think one of the big ways we can educate consumers is to open their mail. So when you get that explanation of benefits in the mail, don't just sit it down and let it collect a pile and you never get around. Open those right away and look at them, because usually that is the first alert or insight that you have into the fact that somebody is using your information to receive medical services.

That usually comes before a bill comes, and what happens is people throw them on the table or they sit them somewhere and they don't open them up. And then when the bill comes, it's months later now when you actually receive the bill from the provider. So before we even get to what people can do on the back-end, I think as more of a preventative method, start opening up those benefit statements earlier, right away.

RYAN MEHM: That's a great point. Thanks for making that.

NAT WOOD: Well, I just want to reiterate. I think it's worth saying again, because it's not welcome news for most people to read the statement of benefits. They're confusing and it is the sort of thing that's sort of intimidating, but it's the best way to monitor what's going into your medical records and what's being charged to your name. So it really is important.

EUGENIA BUGGS: And if you have a provider like ours, again, as I mentioned about the support, if you get the statement of benefits and you don't understand it, you can contact us. We have actual medical professionals on our staff that can help you go through anything that is confusing or you don't understand on there.

NAT WOOD: So in terms of following up, you want to contact all of your medical providers and ask for your records. And if the provider isn't giving you copies of the records, there are things you can do to follow up and try to get those. It's not an easy process. I mean, that's one of the reasons, in addition to the real danger to your health, it can be challenging to follow up on medical identity theft. After you check your medical records, you want to get in touch with your insurer.

You also should check your credit reports. There could be things that would show up on there. And the challenge with medical identity theft is the first things you can do are check your records, and then you sort of need to work from there to whether maybe other records created in your name are using other information.

RYAN MEHM: Lots of great tips there from Nat and Eugenia. I've got a question here for Laura. And, Laura, you described in your remarks earlier how your office awards grants through the various programs that you guys administer. So can you highlight for the audience a couple of other examples of innovative services or programs to assist ID theft victims that have resulted from the grants your office have provided?

LAURA IVKOVICH: In addition to, for instance, the coalitions that were funded, as an example, one in Minnesota was specifically targeting and focused on serving victims of domestic violence. So they have pointed up ways of scanning for when victims come through their shelters to identify-- in addition to their more basic needs of housing or relocation-- but might they also be

suffering from some forms of identity theft and then to lock down or to help prevent further harm. So that is an example.

Also, one of our coalitions in New York, the Finger Lakes region through Life Span of Greater Rochester-- it's an elder service providing agency, and they have focused obviously on victims of elder financial exploitation, where identity theft is obviously a piece of that. Conservative fraud sometimes can be part of that as well. So they have been focusing and working specifically with those victims, even working with nursing homes and other places to help find where that might be occurring and to lock it down. And to go back to one of the questions from earlier panel about what would you do for older victims of exploitation and identity theft, I would say lock it down.

If you don't have a need to buy a house or a car or a large purchase any time soon, because you are no longer in the market for a car because you don't drive or you're in a nursing home-- you're not going to be using your credit to buy another home or something like that-- I would say credit freeze. But that's just me, and that would be what I would recommend to my family members. But some of the innovative things that you wouldn't typically see in a traditional victim service program might be a co-located victim's service advocate working at the Department of Motor Vehicles.

I think it was Delaware had this unique, innovative aspect of their victim program, so that when somebody presents that's not going to find it on their credit report when they are being vigilant and looking at that three times a year through the different reporting companies, credit reporting companies, they can work through the problems associated when they find it right there, that somebody else is using their name to obtain a driver's license in another state. And then they're not able to get theirs renewed. So there's a victim advocate right there at the point of victimization that can help them through those processes to get it concluded at least and get a driver's license. So that's an example.

RYAN MEHM: Great. Thanks. I have a question next for Nat. And part of the goal of today's conference, as we've talked about today, is taking stock of where we are, but also looking ahead and trying to figure out solutions. And so my question for Nat is, what future enhancements do you envision for identitytheft.gov?

NAT WOOD: It kind of goes back to where we started which is working in partnerships. So it's such a complex environment around identity theft and modern financial services and information. So the first steps for us are working with some of the key players in this space.

The IRS is one of those. We've talked a lot today about tax identity theft. Actually, over the lunch break, we were meeting with some of our colleagues from the IRS. We're working to make it so that the IRS form 14039, the IRS Identity Theft Affidavit, that information can be transmitted electronically from identitytheft.gov to the IRS, which should be a great efficiency.

We're working with the credit reporting agencies on getting people deeper into the process for getting a free credit report from identitytheft.gov. And hopefully, over time, that'll be the first of many ways that we can more closely integrate those systems. And all of these different pieces-- when we talk about medical identity theft, when we talk about child identity theft and some of

these new problems that are really at the forefront now, there's opportunities, working through partnerships, to help solve those.

And I don't mean necessarily just through identitytheft.gov. But we're always monitoring what the latest information is and trying to stay on top of the latest threats and challenges. So that's one of the reasons why a session like what's happening today is so important.

RYAN MEHM: Great. Thanks. I see we have literally one minute left, so I want to just quickly go down the line here and ask each panelist where do you see victims' services and resources heading in the next decade. And Nat kind of just answered that a little bit. So maybe, unless you have anything else to add, Nat, we can go on to Laura and Eugenia.

LAURA IVKOVICH: I think technology has caused those who would commit crimes the old-fashioned way by using technology to create it. And so as technology advances, I think so, too, might our reach to victims in both prevention messaging as well as remediation, is going to be increased I think right now there are-- I believe it's in Miami, Florida. I think there's a pro-bono web site that's working to offer free legal advice online.

So I think we're going to find the technology solution is going to help with what technology has made victims so vulnerable, and that's my hope. And we are trying to invest in technology at the Office for Victims of Crime to help that to be the case for our service providers in the field.

EUGENIA BUGGS: So much of what Laura said, and since I guess I'll give the last word on this, I'll answer that question in a slightly different way. I think that one of the things that I'm personally hopeful of, and I hope that I can speak for this section of the industry overall, is that we will kind of move from a place where we're thinking of identity and these types of services from a place of fear-- like I only have this service or we only need this service because of the fact that we're afraid that our identity's going to be stolen or something negative is going to happen to me-- and that we really start to get to a place where people feel more empowered by knowing where their identity information is going and how it's being used, so that they can ask questions when they're getting services and having to give out information in exchange for their services and say, well, do you really need this information and why do you need it and can I give you something else different.

I think right now the consumer feels relatively held hostage to whoever they're trying to get a service from. And if I'm told you need my social security number, my blood type, whatever, what do I do? If I need to give the service, I'm going to give it to you.

So I hope that just by having more discussions like this that we get to the point where the industry starts to evolve in a way that consumers can feel more empowered to say, this is supposed to be private about me. And so if you need something that should have been considered private, I want to understand what you're going to do with it and how you're going to protect it.

RYAN MEHM: Great. Thanks. And that is the last word for this panel. I want to thank Nat, Laura, and Eugenia. Thank you so much. And now I'd like to introduce Tom Pahl, who is acting Director of the FTC's Bureau of Consumer Protection, who will be giving closing remarks.

[APPLAUSE]

THOMAS B PAHL: Good afternoon, everyone. Glad to see that you've made it to the end. I know acting Chairman Ohlhausen said we're going to do a lot of work, and I know that people have done so today. So it's great to see that we've gotten to the end and we're finishing up.

I'm Tom Pahl. I'm the acting Director of the FTC's Bureau of Consumer Protection. I'd like to thank all of you here today for all of your efforts involving ID theft, including the work of the panelists today, the people in the audience, including those folks who are watching on the webcast, where I was for much of the day as well.

As acting Chairman Ohlhausen remarked this morning, identity theft remains a vexing problem that is proliferating in many new ways. As we heard today, identity theft can result in a wide range of economic and non-economic harm, including existing account fraud, new account fraud, medical identity theft, and tax refund fraud, just to name a few. The FTC has long been committed to protecting consumer privacy and combating identity theft through its law enforcement work, by serving as a clearinghouse for identity theft complaints, by helping victims recover from identity theft, and from our ongoing consumer business education and research and development activities, such as today's workshop.

Indeed, today's workshop is yet another signal the commission will continue to remain on the front lines to help prevent identity theft and assist identity theft victims to recover. It's more critical than ever that the FTC remain engaged in these issues, given the changing nature of identity theft. We examined the current identity theft landscape and learned about the growing emergence of the dark web, where consumer information is routinely bought and sold.

As we saw, sites on the dark on the dark web contain a virtual cornucopia of sensitive consumer information available for sale to the highest bidder in identity thieves. Speaking of identity thieves, we also heard about the challenges and successes law enforcement faces when prosecuting these cases. We heard that the news is not all gloom and doom. International cooperation is making a real difference in some cases. More cooperation, though, clearly is needed.

We then looked at identity theft from a big picture perspective and heard about two particularly problematic forms of identity theft-- medical ID theft and tax ID theft. The harms from medical identity theft, as Ann Patterson and Tammy Fine explained, are far greater than just financial harm, and they're very difficult to quantify and to remedy. Like medical identity theft, tax identity theft also inflicts damaging consequences on its victims, often with serious financial implications. This panel highlighted the need to improve information sharing and collaboration.

It also examined whether existing laws and regulations intended to protect consumer privacy are making it more difficult for identity theft victims to remedy the harms they have suffered. For example, medical privacy laws can frustrate the ability of identity theft victims seeking to clear up false information in their medical files or to resolve billing issues stemming from identity theft. We heard about the impact of identity theft on victims-- financial, health and safety, and

other types of harms. Amy Wang traveled from Florida to eloquently relay her own real-life experience of a cascading series of harms that identity of victims all too frequently suffer.

One takeaway from this panel is that there are often real downstream effects or lost opportunity costs from ID theft that go beyond traditional harms that are so often discussed. For example, identity theft victims have lost security clearances and job opportunities as a result of ID theft. We also heard about ID theft victims who have spent hours trying to clean up their financial affairs following identity theft, such as working on efforts to make sure that problematic items no longer appear on their credit reports.

Consistent with acting Chairman Ohlhausen's call for research, we'd welcome research and data measuring all of these effects and costs so we can develop the most effective public policies to deal with identity theft. Finally, we examined the resources available to identity theft victims. We heard about the wide range of resources in place from government and private sector entities to assist ID theft victims. And specifically, we heard about how the Department of Justice's grants are being used to fund innovative partnerships and programs with non-profits and other entities to help identity theft victims.

This model illustrates how consumers benefit when different stakeholders work together. Today's workshop raised a number of important questions to consider as we plan for the future. What current trends and future patterns do recent statistical data on identity theft reveal? What new forms of identity theft can we anticipate moving forward? And what types of harms will we likely see as a result?

What measures can be put in place to assist prosecutors bringing identity theft cases? How can current resources for identity theft victims be improved? Today's workshop puts in stark relief that, while much has been done to combat identity theft, much more still needs to be done.

For starters, today's workshop kicks off a conversation about how to combat this new era of identity theft. Many of the panelists noted that solutions must involve cooperation and coordination among the federal government and more public-private partnerships. For example, panelists talked about the benefits of ISACs in sharing data about specific threats and attacks and about public-private partnerships-- a lot of alliteration there-- such as the IRS's Security Summit.

Because we know that we can't solve this problem alone, we welcome comments from interested parties and stakeholders about additional ways to address the challenges that we heard about today. Your input will be very helpful in informing the agency's views as to our next steps. Comments are due by June 30, 2017 and can be filed through the workshop comment page on the FTC website.

I'd like to conclude by thanking the workshop team responsible for this terrific event and particularly John Krebs, the FTC's Identity Theft Program Manager, and Ryan Mehm. I also want to thank Lisa Schifferle Nat Wood, and Jessica [INAUDIBLE] from the Division of Consumer and Business Education, Maneesha Mithal, Mark Eichorn, Carrie Davis, Matt Smith, and LaQuisha Hawkins from the Division of Privacy and Identity Protection, Dan Salsburg and Tina Yeung from the Office of Technology Research and Investigation, and Keith Anderson

from the FTC's Bureau of Economics. I'd also like to thank our event planning team, Fawn Bouchard and Crystal Peters, Bruce Jennings from our web team, and Juliana Gruenwald Henderson, and Nicole Jones from our Office of Public Affairs.

Thank you all very much for everything that you've put into this event today, and we look forward to working together with everyone in the future. Thank you.

[APPLAUSE]