U.S. Department of Justice
Office of Justice Programs
Office for Victims of Crime

OVC
Webinar Transcript

Talking Through Identity Theft
A Webinar for the Blind and Visually Impaired

July 31, 2013

Talking Through Identity Theft: A Webinar for the Blind and Visually Impaired

Operator: Ladies and gentlemen, thank you for standing by, and welcome to the *Talking Through Identity Theft* conference call. At this time, all lines are in the listen-only mode. Later, there will be an opportunity for your questions, and instructions will be given at that time. If you should require assistance from an operator, please press *0. And, as a reminder, this conference is being recorded. And I would also like to reiterate the password for the Web portion of the call is capital M as in "meeting," so M33ting, and the "ting" is lower case. And, again, if you are having any issues with that, you can press *0 to reach an operator. I will now turn the conference over to Steve Toporoff at the FTC (Federal Trade Commission). Please go ahead, sir.

Steve Toporoff: Thank you for joining us today. We appreciate the opportunity to present this program for those who are blind, visually impaired, and their advocates and advisors. The program is primarily an oral presentation, so you will want to mute your telephone line. For those who wish to listen only, we recommend that you turn off your monitor, as well as any readers or other devices. For those who would like to view the PowerPoint while listening, you can also follow the program on WebEx. If you are having trouble getting into WebEx, please use the help link given in your invitation e-mail. I am sorry we cannot provide other technical support. Rest assured that a recording of this program and a copy of the PowerPoint we will use will be available after the program for your convenience at ftc.gov/idtheft. You will be able to communicate with us orally during the Questions and Answers part of the presentation when the phone lines will be opened. We would love to hear from you. We will also receive written questions through the Chat screen in WebEx. We will monitor the screen and respond as we are able. We will be starting in just a moment so please hold on.

Lisa Schifferle: Hi, everyone. My name is Lisa Schifferle, I am an Attorney with the Federal Trade Commission's Division of Privacy and Identity Protection. And with me is Carol Kando-Pineda, an Attorney in the Division of Consumer and Business Education. We will be talking to you today about identity theft and our presentation is targeted specifically towards blind and visually impaired consumers and their advocates. I will give an overview of identity theft, and then Carol will talk to you about the FTC's resources and how you can access resources that are specifically targeted towards blind and visually impaired consumers.

What We Will Discuss

Lisa Schifferle: So let us start with identity theft. What are we going to discuss today? And those little chimes you hear will happen in between each slide so that you know when to advance the slides. So, first, I am going to start with an overview of identity theft basics. What is ID theft? How do you protect yourself and your friends and family? And what should you do if ID theft occurs?

Lisa Schifferle: Then we are going to talk about some special topics a little more indepth, including medical identity theft and public benefits identity theft, and look at a couple of populations who have some unique challenges in identity theft, namely children and seniors.

Basic Identity Theft

Lisa Schifferle: So let us start with the basics about identity theft.

What is Identity Theft?

Lisa Schifferle: What is identity theft? For purposes of this conversation, we are going to talk about identity theft in terms of someone else using your personal information to pose as you in order to either fraudulently obtain goods or services, or to conceal their true identity. And what this means is basically someone uses your identity in order to get things, whether it is credit card purchases or medical services or your tax refund. Or they might use it to conceal their identity, for example, if I were arrested and gave someone else's name, or if I had poor credit and gave someone else's name who had good credit.

How Information is Misused

Lisa Schifferle: So, now I want to talk a little bit about how information is misused when it is stolen. And the biggest category of misuse, according to our Consumer Sentinel data, is government benefits identity theft. What this data is, this is all the consumer complaints that the Federal Trade Commission receives from consumers about identity theft, and 46 percent of those complaints in 2012 were government benefits related, most of those related to tax identity theft. So we are seeing a huge increase in tax related identity theft across the board. This is up from about 20-some percent of complaints last year, and more like about 10 percent the year before. So it is a very important trend to be aware of is the increase in tax identity theft.

Lisa Schifferle: The other types of ways that information is misused is credit card identity theft, which accounts for about 13 percent of our complaints, utilities is about 10 percent, bank 6 percent, employment 5 percent, loan 2 percent, and other types of identity theft account for 19 percent, and attempted identity theft 7 percent.

The Impact of Identity Theft

Lisa Schifferle: What is the impact of identity theft? When I first started doing identity theft work, I did not fully appreciate the impact of identity theft. I thought of it more like someone stealing your credit card and your wallet, which is a hassle, but there is a lot more to it than that in terms of the impact of identity theft. It can really impact every aspect of an individual's life. It can lead to denial of credit. If your medical information is stolen, it can lead to denial of medical care or even improper treatment if someone used my medical information and their blood type was in my medical records, if I were rushed to the ER and I get the wrong blood given to me.

Lisa Schifferle: It can lead to denial of public benefits. For example, if someone has stolen your identity and is working in your name, then your disability benefits could be denied because Social Security thinks you actually have ability to work. It can also lead to loss and denial of employment. If your credit is messed up due to identity theft, then an employer may deny you employment, saying that you do not have good credit, as a lot of employers now do check credit. It can even lead to arrest in the case of somebody who has an identity thief who used their identity in order to conceal their identity when they were arrested.

Protecting Yourself From Identity Theft

Lisa Schifferle: So, what can you do to protect yourself and your friends and family from identity theft? In order to answer that question, we need to look at how does identity theft happen.

How Does Identity Theft Happen?

Lisa Schifferle: I like to break that down into old fashioned, what I call old fashioned identity theft, and new high tech identity theft. The old fashioned types of identity theft are the traditional lost or stolen wallets. It can also include dumpster diving or stolen mail. There are cases even where pharmacies have left pharmacy prescription information in dumpsters that has gone floating in the wind.

Lisa Schifferle: Theft by family, friends, and caregivers is another big way that identity theft can happen, and this is something to be particularly mindful of with blind or visually impaired consumers, or if you, yourself, are blind or visually impaired. If you have a caregiver who helps you, you need to make sure that you have a background check on that individual and that they are really trustworthy. There was a story recently of an Oregon caregiver for a blind individual, and that blind individual had given the ATM and PIN to her caregiver in order to help her withdraw money. But, unfortunately, when this caregiver withdrew money for the consumer, she also withdrew money for herself. So each time there was a little some for you, some for me. And this individual consumer lost about $68,000, and the caregiver has now been charged with identity theft. So that is just an example of how identity theft can happen in the caregiver context.

Lisa Schifferle: Another way it can happen is through a corrupt insider. We know that there are insiders going into nursing homes and assisted living facilities and hospitals, and they are being paid to take information from the nursing homes, people's personal information, in order to perpetrate identity theft. So those are some of the more old fashioned forms of identity theft.

Lisa Schifferle: In addition, there are a lot of high tech ways, now that everything is online, that people can steal your identity. There are data breaches. Many companies, including companies such as T.J. Maxx that many people may shop at, have had data breaches where they have lost consumer credit card information.

Lisa Schifferle: There are phishing scams which basically means somebody calls or e-mails you and asks for your bank account information or other personal information. They pretend to be legitimately from your bank or elsewhere, and ask you to give over your personal information. And, in fact, they go on to use it for identity theft purposes.

Lisa Schifferle: And malware, finally, is another form of high tech identity theft. You need to be very careful when clicking on links in e-mails, not to click on links in e-mails, especially in unsolicited e-mails because they could install malware on your computer that then can take your personal information.

Deterring Identity Theft

Lisa Schifferle: So now that we have talked about how ID theft happens, we can move on to how to deter it and how to keep it from happening. There are a few tips that we like to give people. One big tip is to empty your purse or wallet. Do not carry around everything under the sun in your purse and wallet, and particularly do not carry your Social Security card with you. When you are done with documents with personal information, it is very important to shred them and dispose of them properly.

Lisa Schifferle: Another tip, which I discussed earlier, is to make sure to select assistants, advisors, and caregivers very carefully. And in order to prevent phishing scams, which I

mentioned, you do not want to give out your personal information unless you are sure you know who you are dealing with. If someone calls or e-mails and says they are from your bank, I just got a call yesterday from someone who said they were from my mortgage company. Make sure you know they really are from the mortgage company and call them back on a number you know to be the mortgage company, not at the number they give you. And verify who they are before you give any personal information.

Lisa Schifferle: The best way you can deter identity theft is to monitor your accounts and to get your free annual credit report. And I want to remind people that the best place to get your annual credit report is at www.annualcreditreport.com. There are a lot of copycat sites that sound similar, but www.annualcreditreport.com is the one legitimate site to get your annual credit report from. And, fortunately, www.annualcreditreport.com has some special services for blind and visually impaired consumers. You can request internet-based audio, Braille, and large-print credit reports at www.annualcreditreport.com, or you can call them at 877–322–8228. Again, that is 877–322–8228, and you can get your credit report for free and confidentially, and an internet-based audio or Braille or large-print version.

Lisa Schifferle: So that is some of the ways you can protect against some of the more old fashioned and even some of the high tech types of identity theft. But to really protect against high tech types of identity theft, we need to talk briefly about online safety and some tips for that.

Online Safety

Lisa Schifferle: So, some of the big things you can do to protect yourself online are to keep the anti-virus software on your computer up-to-date so that you can stop malware and other viruses from coming onto your computer. Be careful of using social networks, and if you have teenage children or grandchildren, it is important to teach them as well not to share everything under the sun on social networks, and not to share things like your full date of birth, including year, not to share things that would allow people to guess your passwords. Like if your security code question is, "What is your high school mascot," and you can go on your Facebook account and see what high school you went to, then anyone can guess your password and get your password into your account. So be careful what you share on social networks, and also use difficult to guess passwords, and difficult to guess password security questions.

Lisa Schifferle: I already mentioned do not click on links in unsolicited e-mails because they can install malware or viruses. And another huge thing is a lot of us like to do shopping online, and when we shop online it is very important to make sure the site that you are using is secure, and the easiest way to do that is to look for the little lock symbol or it would have https at the beginning of the website, instead of http, it should be https. So, hopefully, even a screen reader could read that for you to notice if there is the "s" at the end of the https.

What to do if Identity Theft Occurs

Lisa Schifferle: So, what do you do if identity theft occurs? Because you can take all these prevention steps and still be a victim of identity theft, or maybe you will take them but someone in your family will not, and they will become a victim of identity theft.

Four Steps

Lisa Schifferle: We break down what you should do if you are a victim into four steps. The first step is contacting the consumer reporting agencies (CRAs). The second step is contacting the

companies where the fraud occurred. The third step is filing a complaint with the FTC. And the fourth step is filing a police report. And I will go through each of these steps in turn.

Step 1: Contact CRAs

Lisa Schifferle: Step one, contact the credit reporting agencies. Now, what I mean by the credit reporting agencies are Equifax, Experian, and Transunion. Those are the big three credit reporting agencies that are responsible for generating your credit report. You can contact them by phone or online, and this information is available in the PowerPoint so do not be worried if you cannot write it down as I am saying it now. But I will tell you the contact information for Equifax is www.equifax.com, and their phone number is 800–525–6285. Experian is www.experian.com, and they are at 888–EXPERIAN. And Transunion is at www.transunion.com, or 800–680–7289.

Lisa Schifferle: So you want to contact the credit reporting agencies and what you want to do when you contact them is place a fraud alert on the credit report. You also should ask for a copy of your credit report free of charge so that you can check and see exactly the full extent of the identity theft. You may be aware of the thief having misused your credit card at Target but may not be aware of all the other ways the thief has misused your credit card or other personal information, and the credit report is a good way to get a full picture of the damage that is being done by the identity theft.

Lisa Schifferle: So the other big thing you want to do in Step 1 when you are contacting the credit reporting agencies is to place a fraud alert or a credit freeze. And I will explain what each of those are.

Fraud Alert

Lisa Schifferle: A fraud alert basically means that creditors have to take reasonable steps to verify your identity before any new credit is extended. So if someone is at a car dealership saying that, you know, they are you and they want a loan, then you should get a call saying, "Is that really you, and can you verify that it is you," before any new credit is extended to that individual. In order to place a fraud alert, you only need to make one call. You only need to call one of the three credit reporting agencies, Equifax, Experian, or Transunion. And they have an obligation to notify the other two of the fraud alert. The fraud alert is free and it lasts for 90 days. You can also get an extended fraud alert for 7 years under certain circumstances.

Credit Freeze

Lisa Schifferle: You may also want to consider a credit freeze. And a credit freeze…And there was no chime for some reason between that slide, but I did just advance the slide between the Fraud Alert slide and the Credit Freeze slide. So the credit freeze is – basically means that your credit is frozen both to you and to other individuals, so nobody can apply for new credit, not even you, until your credit is unfrozen. What happens is you will get a little PIN number and your credit will be frozen. If you want to unfreeze it, you will need to use that PIN to unfreeze it. And the credit freeze is governed by state law, so depending on what state you are in, there may or may not be a fee for placing the credit freeze. And there may or may not be a fee for each time that you unfreeze the account. So that is something to consider is whether your state has fees for the credit freeze, and many states waive those fees if you are an ID theft victim, so do not assume that you are going to have fees and decide not to do it because of that. But that is just something to look into is what are the fees?

Lisa Schifferle: And, also, do you need access to credit? If you found out about this identity theft because you were applying for a mortgage and then you found all these problems on your credit report, you may not want to put on a credit freeze right then because you are still trying to get credit yourself and it is going to be a hassle and inconvenience. If you are someone who is in a position in your life where you have taken out most of the credit that you expect to take out, then a credit freeze might be a good option for you because it is more secure than the fraud alert in many respects.

Lisa Schifferle: So that is Step 1 of what to do if you are an ID theft victim. Step 1 is contact the credit reporting agencies, get your credit report, and consider a fraud alert or credit freeze. Let us move on to Step 2.

Step 2: Contact Companies Where Thief Committed Fraud

Lisa Schifferle: Step 2, after you have contacted the credit reporting agencies, is to contact the companies where the thief committed fraud. For example, if someone took my credit card and shopped at Giant Eagle and Target, then I would need to contact Giant Eagle and Target, and contact their fraud department and tell them to close or freeze the accounts that have been fraudulently opened. If someone opened an account that you never had, then you may as well close it because there is no concern about having a long-established line of credit that you do not want to close out. It is a completely fraudulent account and you can close it out.

Lisa Schifferle: So once you have contacted those companies, you will want to send them a written dispute, including an identity theft affidavit. And we will talk in Step 3 and 4 about how you create that. But, basically an identity theft affidavit consists of a police report plus your FTC complaint printed out in affidavit form.

Lisa Schifferle: So when you contact the companies, you are going to talk to their fraud department, ask them to close or freeze the account, and then request a letter from the company describing the results of their actions.

Step 3: File a Complaint with the FTC

Lisa Schifferle: Step 3 is to file a complaint with the FTC. The reason to do this is not only because we track ID theft complaints and we can go after perpetrators who are going after people in large quantities, but also because it helps you as an individual because you can print out your complaint as an ID theft affidavit and you will have all the information you need in one place in order to exercise certain rights under the Fair Credit Reporting Act (FCRA) to clean up your credit report. And it may even help you to file a police report, especially for someone who is blind or visually impaired, it could be helpful to have this complaint to hand to the police, and then the police can basically say "see attached" for their police report. It makes the police's job easier and then you know what is going into the report.

Lisa Schifferle: So, to file the complaint with FTC, you can call 877–438–4338. And we also have hotline phone counselors who are trained in identity theft and can walk you through a lot of the steps that you would need to take. We also have a web-based complaint filing system, which is available at www.ftccomplaintassistant.gov.

Step 4: File a Police Report

Lisa Schifferle: Step 4 is to file a police report. You should call the local police as soon as possible after you become aware of the identity theft in order to report the ID theft. A special note, which we will go into more when we talk about child ID theft, is that the police report might not be as critical for children if a child is a victim of identity theft. Because rather than having to exercise their rights under the Fair Credit Reporting Act and having to show that they are not the identity thief, they can just show, "I am a kid, I am a child, and I am below the age of majority, so I do not have capacity to contract," because children are not allowed to enter into contracts by law. So if there is something on a kid's credit report, then you know, if it is a kid, it could not have really been theirs. So for a child, filing a police report may not be as critical. But for adults who are victims of ID theft, Step 4 is to file a police report.

Lisa Schifferle: So, just to review, before we move on to the special topics, the four steps to take if you are an ID theft victim are: 1) contact the credit reporting agencies, 2) contact the companies where the thief committed fraud, 3) file a complaint with the FTC, and 4) file a police report.

Special Topics

Lisa Schifferle: Now, I want to move on to some special topics because another area of increasing concern is medical identity theft.

Medical Identity Theft

Lisa Schifferle: Medical identity theft can involve the thief using your identity or health insurance to receive care. It may happen by somebody getting your wallet with your health insurance card, or they may get information through a data breach. And medical identity theft can be extremely harmful because the thief's medical records may become merged with your medical records, and as I mentioned before, it could lead to denial of treatment or improper treatment. It also can be very difficult to remedy because unlike the financial account ID theft which I talked about earlier in terms of the four steps, there is no central repository like the credit reporting agencies, there is no one place to go in order to clean up medical ID theft.

How to Assist Victims

Lisa Schifferle: So what do you do if you are a victim of medical ID theft, or if you know someone who is? The way to assist a victim of identity theft that relates to medical records is you still do want to report the theft to local law enforcement, but you also want to request medical records and the privacy policy from your regular provider, as well as from each provider that gave care to the thief.

Lisa Schifferle: And one tip that is often told by advocates who assist medical ID theft victims is do not mention the ID theft initially when you are requesting the records. And why is that? Because if you do, you may accidentally or inadvertently invoke the imposter's HIPAA rights. There are certain privacy protections, and a medical provider may correctly or incorrectly, if you say, "I am a victim of ID theft, I want my medical records," they may challenge, saying, "Are you really you or are you the ID thief? I do not know if I am going to give you the records." But if you just call and say your name and say you are requesting your records, there is no reason for them to challenge your identity. And then once you have your records, then at that point you can compare them and look at them and correct them, and then write back to the provider and say, "I

see these records, this was not care that was rendered to me, I am a victim of ID theft and I want you to correct my records."

Government Benefits Identity Theft

Lisa Schifferle: So the next special topic that I am going to talk about is government benefits identity theft, and then we will talk a little bit about child identity theft and senior identity theft.

Lisa Schifferle: As I mentioned near the start of the presentation, government benefits identity theft is now by far the leading type of ID theft complaint that we receive at the FTC. How does it happen? It can happen in a variety of ways. The thief may file a tax return using your Social Security number in order to get a tax refund. This is a very common scheme that a lot of organized crime gangs that used to deal in drugs are now dealing in tax refunds and ID theft. It can also happen is a thief or even someone you know claims your child as a dependent on the tax return, and then you are not able to claim them.

Lisa Schifferle: Finally, another common way it happens is if a thief uses your Social Security number to get a job and earn money, and then you may get a notice from the IRS saying that you have not paid taxes on all the wages earned. It may also lead to disqualification from disability benefits if you are receiving disability benefits and you are working, or they think you are working because of the identity thief's work, then it may – you may be disqualified from disability benefits.

Lisa Schifferle: And next, the thief may apply for public benefits using your personal information. These types of public benefits ID theft are especially prevalent in long-term care facilities in Florida and Georgia.

Resolving Benefits Identity Theft

Lisa Schifferle: So what do you do if you are a victim of government benefits identity theft? Well, there are a few things that you can do. First, you want to get a copy of your earnings record from the Social Security Administration. You can do that either by going into your local Social Security office and requesting it, or now, in the past year or so, Social Security has also made it very convenient for you to get your earnings statement online at socialsecurity.gov/myaccount. So you want to get your earnings record and then see is there earnings on there for earnings that you did not do? For example, if I saw earnings on my earnings record for someone who worked as a waiter in Texas, I would know that I do not live in Texas and that was not something that I earned. And then I would go and mark the imposter activity on my earnings record, and provide the corrected earnings statement to Social Security, request that they correct my earnings record, and that my Social Security number be flagged.

Lisa Schifferle: In addition, since we know that tax identity theft is such a big and growing problem, I would strongly suggest to anyone who knows that their Social Security number has been exposed to contact the IRS's Identity Protection Specialized Unit, and they can flag your Social Security number for tax purposes and even give you a special PIN to file under, rather than filing under your Social Security number. And the IRS's Identity Protection Specialized Unit can be reached at 800–908–4490. And I have heard from a lot of advocates that the IRS Specialized Unit is very responsive and very helpful. So I do encourage people to use that resource.

Child Identity Theft

Lisa Schifferle: The last couple of topics we are going to talk about before hearing about consumer education resources are child identity theft and senior identity theft. Because when a child or a senior is a victim, there are a few other considerations that may come into play. And, for this reason, the FTC has hosted forums both on child identity theft and senior identity theft. If you are interested in learning more beyond this presentation, both of those forums are available to be listened to and watched on our website at www.ftc.gov, if you just look for the Stolen Futures Forum and the Senior Identity Theft Forum, you can learn more. But for now, I will give you the basics on child identity theft.

Children are Vulnerable to Identity Theft

Lisa Schifferle: First, why are children vulnerable to identity theft? Some studies show that children are victimized at a much higher rate than adults in terms of being identity theft victims, and it makes sense, if you think about it. Kids have clean credit, which is appealing to an identity thief. They know if they steal a kid's credit, they are getting credit that has not been used, as opposed to if they steal an adult's credit, the adult may have already ruined their credit through their own credit habits.

Lisa Schifferle: In addition, children's information is readily available. It is often available in a lot of contexts, like schools, pediatricians' offices, sports clubs, and other places that may not be able to put the highest degree of security on that personal information.

Lisa Schifferle: Finally, thieves know that if they steal a child's identity that the theft is likely to go undetected for years because most people do not check their children's credit.

Deterring Child Identity Theft

Lisa Schifferle: So what should you do to try to deter child identity theft? It is a lot of the things that we talked about in terms of deterring adults' identity theft. You want to protect what you have. Keep all of your personal items safe and secure, both online and paper.

Lisa Schifferle: Be careful what you share. Do not give out the information unless the person really needs it. A lot of places ask for kids' information that does not need as much information as they request.

Lisa Schifferle: Talk with children. Talk with them about online safety. Talk with them about sharing personal information.

Lisa Schifferle: And, finally, safely dispose of personal information of children, and make sure that their schools and their pediatricians' offices are doing that as well.

Monitoring a Child's Credit

Lisa Schifferle: Now, a lot of people when they hear about child identity theft get worried that kids are victimized at such a higher rate and say, "Should I run out and check my child's credit today and every year from now on?" We do not necessarily think that it is necessary to check a child's credit every year unless you have some reason to believe that your child's information is at risk. Certainly, if you know your child was part of a data breach or if you know that there is

somebody close to them or suspect there is someone close to them that may have misused their personal information, you should check it every year. But otherwise, for most people, it is probably sufficient to order a credit report some time close to the child's 16th birthday or some time a couple of years before you think the child may first need access for their credit, either for student loans or a car loan or some other purpose. You want to do it enough in advance so that you have time to clear up any errors before the child, themselves, needs the credit.

Lisa Schifferle: And, you should know that when you check a child's credit, if there is anything on the credit report, then there is a problem because the child should not have anything on their credit report. One tip we give people is do not use www.annualcreditreport.com for children. I mean we tell people over and over again. For adults, make sure you use www.annualcreditreport.com, and that is true. For adults, that is the one site to use, www.annualcreditreport.com. But for children, that will not work as well. Instead, we recommend calling each of the credit reporting agencies individually and asking for what we call either a manual search or a Social Security number only search. What this does is then they will check for any credit records under the child's Social Security number. Because we know in child identity theft oftentimes, most often, thieves are using the child's Social Security number in conjunction with their own name or a made up name. So if you just do a regular credit check, they are going to look for the child's name in connection with the Social Security number and they may miss a lot of incidents of child ID theft, which is why for children we do suggest asking for a manual or Social Security number only search.

Contacting CRAs for a Child

Lisa Schifferle: A couple of other tips for children. Not only is there a different method for requesting the credit report, but there is a different response if you find problems on the credit report. As I alluded to earlier, since a child is a minor under the age of 18 in most states, they cannot by law enter into any contract. So anything on their credit report should be – is an error. So rather than providing proof of identity and proof that they were not the one that took out the charges, you should be able to simply provide what we call a Uniform Minor's Status Declaration, which is just a form that we have created and that you can find in our publication called *Safeguarding Your Child's Future*, which Carol will talk about later. You can provide the Uniform Minor's Status Declaration to the credit reporting agency, and what that does is basically just says that this person is a child. And you attach a copy of the birth certificate as well to prove that the person is a child, and by virtue of that, that everything on the credit report is wrong and should be removed. So you would, with Uniform Minor's Status Declaration, request that the CRA, the credit reporting agency, immediately remove all accounts, application inquiries, and collection notices from the child's file.

Senior Identity Theft

Lisa Schifferle: So next we are going to talk about senior identity theft. Now, for children, as I mentioned, the techniques for getting their credit report is different and the solutions if they are a victim are different. For seniors, seniors are just another type of adult, and so the methods for both requesting a credit report and for correcting the credit report are the same as the ones I went through earlier. You still use www.annualcreditreport.com and you still use the four steps I discussed earlier. What is different for the most part with seniors is they have very different vulnerabilities.

Identity Theft and Seniors

Lisa Schifferle: With seniors there are three common perpetrators: relatives, caregivers, and scammers. And seniors may be more vulnerable to identity theft because many people have access to their information. Some seniors may be more likely to go to a variety of doctors and have their information in more places. We know that scammers target long-term care facilities and assisted-living facilities for seniors who are in those facilities. And even for active, independent seniors, many seniors have built wealth over their lifetime so they are attractive targets for identity theft – for identity thieves.

Lisa Schifferle: And there are special considerations when the thief is a relative or a caregiver. Some people may be more reluctant to file police reports against those individuals. But they should know that only if they file a police report that enables them to exercise all of their rights under the Fair Credit Reporting Act, which helps them to block certain information from their credit report.

Reporting for Seniors

Lisa Schifferle: One other special tip in terms of seniors is the reporting requirement for seniors. For seniors, the ID theft affidavit can be signed by a personal representative. It can, you can attach a power of attorney or guardianship letter to it. And, in addition, for the police report, any interested person can make the law enforcement report on the senior's behalf. So this really only comes into play for seniors who may have diminished capacity, and in those cases you may want to consider these additional considerations for reporting for seniors. The senior does not always have to report themselves. You can do it through a personal representative or an interested party for the law enforcement report.

Lisa Schifferle: And, as I mentioned before, the steps for seniors are the same as for other adults. To monitor for ID theft, you want to check www.annualcreditreport.com. And if you are a victim and you want to take the four steps. First, contact the credit reporting agencies. Second, contact the companies. Third, contact the FTC. And fourth, contact the police.

Lisa Schifferle: So that is my overview of identity theft, and now I am going to turn it over to Carol who is going to talk to you about our consumer education resources. And at the end of her presentation, we will have time and open the lines for questions. So here is Carol.

Consumer Education Resources

Carol Kando-Pineda: Okay, thank you, Lisa. And thanks, everybody, for giving us a little bit of your time this afternoon. I am going to walk you through some of the special resources that we have for identity theft and ones that might be especially useful for folks that are blind, visually impaired, or the folks that work with them.

Carol Kando-Pineda: So, first, I am going to walk you through basically two sites, consumer.gov and ftc.gov/idtheft. So let us start with consumer.gov. That is our site that has got a lot of our consumer information on it, but in a very pared down form. It is just the basics. We have been told by many people that our information is very helpful, but sometimes it is just a little overwhelming, it is too much. There might just be one or two points that you need to get and this is the site that is designed to do that. So it has different components, there is a website, print

materials, read-along audio, simplified video, and then there are some resources for community leaders.

Carol Kando-Pineda: So, if you get on to consumer.gov, across the top of the screen you will see three tabs. You want to click on the third one, that is Scams and Identity Theft. So when you get to the next screen, there are five links in the center of the page. The first two relate to identity theft, they are Avoiding Identity Theft and Recovering From Identity Theft.

Carol Kando-Pineda: So, under either one of those…Obviously the Avoiding Identity Theft is a protection piece and the Recovering is the steps that Lisa just walked you through in a very simplified format. So each of those topics is broken down into "What it is," some basic definitions, some basic explanations; "What to know," just the core things that you really need to know; and "What to do." Are there any action steps that you need to take to either be sure you lock down your information or to recover if you become a victim? All right, so you are going to see those tabs across the top: "What it is," "What to know," "What to do." You can click on any of them and sort of walk through and see what the materials are.

Carol Kando-Pineda: When you get to any of those screens, there is a read-along audio. So every single bit of that article for "What it is," "What to do," "What to know," has accompanying audio to go along with it. So to access that, you want to go to the left of the screen and click on the speaker icon. Now, another way to do that is to go to the very bottom of the screen and there is a play button, a little triangular play button that you click. Either way, you can hear the audio or you can turn it off. And that may not suit everybody, but if it does, it is a nice little addition to be able to hear every bit of the article.

Carol Kando-Pineda: So, say you have become an identity theft victim or you are assisting somebody that is an identity theft victim, or you just want to know more about identity theft, maybe you want to even host an event and share some materials in your community about identity theft. Then I would suggest that you go to our main identity theft site which is ftc.gov/idtheft. So there you will be able to drill down and get a little bit more detailed information. So this site has got a little bit more going on, but it is our main topic page for identity theft, and there is a series of links down the center of the page. It basically divides identity theft into some smaller sub-topics: what you need to do immediately, what to do next, specific types of identity theft, protecting your identity, and sample forms and letters to help you.

Carol Kando-Pineda: So that probably sounds a little bit familiar. It is a lot of information that Lisa has walked you through already. And if you want to learn more about that, get onto that page and click through the links that are under any one of those sub-topics, and they take you to the relevant article.

Carol Kando-Pineda: So another thing I want to point out is head on over to the right side of the screen to the navigation bar. Click on the second box, that is Free Resources. Just a little box, Free Resources. If you click on that, it takes you to a different screen that has got all the different materials that we have that you can either download or order for free from our bulk order website.

Carol Kando-Pineda: So the first thing there is our Outreach Toolkit. That includes everything that you would need if you wanted to host your own kind of an event. So talking points, sample slide presentations, sample newsletter articles, social media, press release. All that stuff is there if you wanted to sort of take this stuff and go out into the world and spread the word on your own.

Carol Kando-Pineda: Also in that section there is a link to the slides from this Webinar and the audio from this Webinar. It will be identified as, I think it is *Talking Through Identity Theft*. But you will be able to tell, that link will be right there and then the audio will be right beneath it.

Carol Kando-Pineda: All right, so to just repeat that quickly, you want to go to ftc.gov/idtheft. Click on the Free Resources button at the right. And then under Spread the Word, you want to click on *Talking Through Identity Theft* or click the link that is below that to listen to the audio.

Carol Kando-Pineda: Also on this page you will see a link to *Taking Charge: What to do if Your Identity is Stolen.* That is our great big resource book about recovering from identity theft. That covers pretty much everything you need to know about recovering from identity theft, including some sample letters and forms that will get you started.

Carol Kando-Pineda: There is also the book that Lisa was referring to, *Safeguarding Your Child's Future*, which will walk you through all the steps that need to happen if you suspect your child's identity has been stolen, or if you want to do that manual search with the credit reporting companies to be sure that your child is protected.

Carol Kando-Pineda: And one of the other pubs that I wanted to point out to you is the trifold brochure. It is kind of somewhere in between the just the basics that I first described on consumer.gov and the big booklet, *Taking Charge*, that is on ftc.gov/idtheft. *ID Theft: What to Know, What to Do* is a two-page brochure. It is one page, two sides, and it just gives you a good overview with a little bit more detail. If you only wanted to pick up one thing, it is a really helpful item to have. What is interesting about this one is we have had a couple of different versions. So we have got a version with a few extra tips for service members and military families. It comes in Spanish and also Chinese, Korean, Tagalog, and Vietnamese, which was kind of a first for us but we were able to do that and happy that we could offer it to folks.

Carol Kando-Pineda: All right, so one more thing I wanted to walk you through is the rest of the materials the FTC puts together about other kinds of topics, credit and debt and job scams, and also other topics related a little more peripherally to identity theft, and that is at consumer.ftc.gov. That is our consumer center, consumer.ftc.gov. So if you go to that site, across the top are the words Consumer Information. Below that are six tabs. You see the last one has got two choices, Blog and Video & Media. So if you click on Video & Media, that takes you to our entire collection of audio clips and videos that you can listen to for quick tips on a wide variety of issues. So, the videos run a little bit longer sometimes. Some of them are a minute and change. Some of them are a little bit longer. The audio clips are all just 1 minute. So they can be really a nice, quick hit if you just want some tips about a topic, very easy to use. If you want just the video or just the audio, you can also get to them by going to the search box that is at the top of any screen on the website, and type in "audio." The first link in your results says, "Got a Minute?" Click on that. That is all of the audio tips combined onto one page, if that is all that you wanted.

Carol Kando-Pineda: So if you want a copy of our materials, whether to use for yourself or to give out, whether on identity theft or other topics, you can download the identity theft information from ftc.gov/idtheft or you can order free copies of any of our resources at bulkorder.ftc.gov.

Carol Kando-Pineda: Now, we also do have this one special product that is a CD of all of the audio files that we have compiled and put into one spot, if you would rather not have to navigate and get them online. If you would like a copy of that CD, you can e-mail our colleague, Cheryl

Thomas, here at FTC at cthomas@ftc.gov. And so I think that is the basics that you need to know about getting materials from FTC, and I am going to turn it back to Lisa.

Questions and Answers

Lisa Schifferle: Thanks. Now we are going to go to Questions and Answers. Before we open the lines for questions by telephone, I just want to answer a couple of questions that have come in through our Chat function. The first question says: Recently I have had my birthdate modified on my credit history. This was resolved by contacting each bureau. How can anyone modify fixed information on my credit history? I cannot even wonder how such data could be changed.

Lisa Schifferle: Well, there are a couple of ways that that data may be changed. It may be just a mistake. It may be a mixed credit file with someone else's who has a similar name or birthdate. It may be someone who transposed numbers accidentally. Or it could be an identity thief using your information. The important thing to know is that if you do have mistakes on your credit report, there are two different ways that you can remedy them. The first is to do what we call blocking, which is a right under the Fair Credit Reporting Act section 605B, and basically you write to the credit report if you are a victim of ID theft, and you will need to include a copy of a police report in order to exercise this right. And within 4 business days they are required to remove that information.

Lisa Schifferle: The second way you can address mistakes on your credit report is through the regular dispute mechanisms, and this is a right under the Fair Credit Reporting Act section 611. But you do not need to know the FCRA numbers when you make the request. You can just write in saying that you dispute the information, and if you do want the exact sites, you can look at our publication, *Taking Charge*…[background conversations]

Lisa Schifferle: I hear somebody on the line who is not muted. Can the AT&T operator please try to address that situation, please?

Lisa Schifferle: So, the two ways to address mistakes on the credit report are through blocking or disputing. And if you dispute, you just write in saying you have a dispute. The credit reporting agency has 30 days in order to try to correct it.

Lisa Schifferle: The next question we have through our online Chat function is: My doctor's office medical records told me that I had to pay for any pages in excess of 100 pages. My chart is more than 250 pages long.

Lisa Schifferle: Well, when you request medical records, it is likely that you will have to complete a form and you may have to pay a fee to get a copy of your record. Under HIPAA, the doctors' offices and medical providers are required to give you your files within 30 days after you ask for them. Whether the degree of the fees may be governed by state law, you may want to check your state laws on that. But if a provider refuses to give you access to your records within 30 days of your written request, you can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights, and you can do that at www.hhs.gov/ocr.

Lisa Schifferle: So those are the two questions we have gotten through our Chat function. Now, if the AT&T operator could please open the lines and we will take questions verbally.

Operator: Certainly. If you would like to ask a question, please press *1 on your telephone keypad. You will hear a tone indicating you have been placed in queue, and you may remove

yourself from the queue at any time by pressing the # key. If you are using a speaker phone, please pick up your handset before dialing. And our first question is from Cliff Jones with Blinded Veterans. Go ahead, please.

Cliff Jones: Yes, I would like to know, you gave out a number earlier about the annual credit report, but you gave out a telephone number that you can call and I guess have it where you can have it where you can get it reading from – I use JAWS, I want to be able to read it with JAWS.

Lisa Schifferle: Okay, yes. You can request an internet-based audio, Braille, or large-print copy of your credit report. And the phone number to do that is 877–322–8228. That is 877–322–8228. And, again, it should be a free credit report even if you are requesting it in an internet-based audio, Braille, or large-print version.

Cliff Jones: One quick one. Is there any special time of the year that I need to request that?

Lisa Schifferle: No, you can request it at any time. You are entitled under law to one free annual credit report per year from each of the three credit reporting agencies. So if you wanted to, you could space it out and this month get one from Experian, and 3 months from now get it from Equifax, and 3 months from then get it from Transunion, or you could get them all three at once. But you are entitled to one free per year at any time during the year.

Cliff Jones: Thank you.

Lisa Schifferle: Thank you.

Operator: Our next question is from Myra Schiff with the Jewish Guild Healthcare. Go ahead, please.

Myra Schiff: I would like to know if all of your sites and screens are accessible through voice output software such as JAWS and ZoomText and MAGic?

Lisa Schifferle: We are not sure about that. I would think that they would be compatible with them, but we do have a lot of audio files. Our consumer.ftc.gov site is audio ready and we have collected all the audio files on a CD which, again, you can get a copy of by contacting Cheryl Thomas at cthomas@ftc.gov.

Myra Schiff: Thank you.

Operator: Thank you. Our next question is from Donna Myers with no affiliation. Go ahead, please.

Donna Myers: Yes, I have two quick questions. My first question is, when I get my annual amount of my disability check from the Social Security office, and it comes in the mail, it includes my full Social Security number. And I have tried to talk to them about that and they said there is no choice, that is the way it comes. I do not like my Social Security number being laying out in the mailbox. And my second question would be, I have a granddaughter who I have created some accounts for to save her some money for her education, and her, her father is incarcerated and there are some issues with her mother. And do I need to keep a check on her in any way and do I have the right to do that?

Lisa Schifferle: Okay, let me start with your first question about your Social Security number and not wanting to have it in your mailbox and on your checks as they come to you.

Donna Myers: It is not my checks, ma'am. It is the annual credit report.

Lisa Schifferle: Oh, on the annual credit report. Oh, okay. All right, well, the annual credit report is…

Donna Myers: It is not the credit report. It is the annual amount that I get every year.

Lisa Schifferle: The annual statement of…?

Donna Myers: Yes, ma'am. My income for the year.

Lisa Schifferle: Okay, well, Social Security, you can sign up to get those statements online instead of having them come in your mailbox, at socialsecurity.gov/myaccount. Then you do not have to worry about them coming in your mailbox, and it may be more secure that way. In terms of your granddaughter, it sounds like from the situation you described that it would be worthwhile keeping an eye on what is going on with her accounts. If they are accounts that you have set up for her and you are the custodian of the accounts, then you ought to be able to monitor them. If there are other accounts, then it would depend on, you know, who has custody or guardianship of your granddaughter, whether there is a right to access information relating to them.

Donna Myers: Well, they are her accounts. I mean I am, you know, the "co" on them. But I mean could her mother or father steal her identity in any way?

Lisa Schifferle: Sure. I mean anyone could steal her identity, and if you have reason to believe that, you know, someone close to her might, then that is all the more reason to check her accounts more regularly and to try to check her credit reports regularly as well. Now, I see it is 3:00 o'clock, but we will stay on the line to answer a few more questions if the operator could give me the next question, please.

Operator: Okay, that will come from Bob Burnham, also with no affiliation. Go ahead, please.

Bob Burnham: Hi, and thank you for your presentation today. What is your take on advertised identity theft websites like ID Guard and LifeLock and things that are highly advertised in terms of protecting identity theft?

Lisa Schifferle: Well, we warm consumers to be very wary of any commercial identity theft protection services, and to check what it is that you are paying for, because there are many of these services that make you pay for things that you could do for yourself for free. In addition, some of these services, like LifeLock for instance, we have sued and put under order for their deceptive practices. So you may want to check on www.ftc.gov to see if the identity theft protection service that you are considering is one that we have sued for deception or unfair practices. And also, even if it is not, still be wary of it. And we actually have a publication on our website specifically on identity theft protection services and what to look at and what to consider if you are considering purchasing them.

Bob Burnham: Thank you.

Lisa Schifferle: Thank you.

Operator: Our next question is from Greg Rosenberg with Reese's Incorporated. Go ahead, please.

Greg Rosenberg: Sure. I just want to follow up on my one question I posted earlier. Your birthdate, your Social Security number, the spelling of your name are things that are rather permanent. I am 57 years old. I have had the same birthday for 57 years. It strikes me as extremely odd that a third party could submit a record that could alter that data. And I am just trying to understand what steps that need to be taken in order to, you know, create legislation or create guidelines to avoid that type of situation. I am not only thinking of myself, but many other people I know that have had fraud or identity theft committed against them. And, in many cases, they have had data in their personal record altered. So since there is – since at least one of you is an attorney, I thought maybe there are some thoughts there.

Lisa Schifferle: Well, I cannot comment on legislation or guidelines, but I can tell you that there are laws in effect, the Fair Credit Reporting Act, specifically, that help address such mistakes in your credit history. And as I mentioned before when initially responding to the request, there are two different ways you can address those mistakes. One is through blocking that information under FCRA 605B, for which you need a police report. And the second way is to dispute that information under FCRA 611 and just say, "This is not my correct birthdate," and provide a copy of your birth certificate and ask for it to be corrected. I mean, certainly people make mistakes, computers make mistakes and people make mistakes, so it would be easy for a birthdate, even though it has been, you know, the same over the years, there are years – all those years that someone could have made a mistake and typed it in wrong or entered it wrong or mixed it up with somebody else. So mistakes happen but there are ways to correct them if they are through the Fair Credit Reporting Act, as I described.

Greg Rosenberg: My understanding in talking to the credit bureaus is they are allowing updates from third parties of any of that information. Someone could actually, you know, give them my Social Security number, they could even update or change my Social Security number in the credit bureaus' databases. And I have been working with credit bureau databases through a lot of my customers' banks and mortgage companies for many decades and this has really been an ongoing problem for a long time that, you know, third parties can submit inaccurate information that is not verified, that overrides data in the credit bureau. And then it requires, you know, someone to either have a bad experience as a result of a difference in the birthdate they have put down or Social Security number, or even spelling of their name in some cases.

Lisa Schifferle: Right, I mean certainly, I mean those mistakes, that is why one of the main functions of the Federal Trade Commission is to bring law enforcement action against companies or entities that violate the Fair Credit Reporting Act. So we are mindful of those types of issues and we do take both enforcement actions and do consumer education to try to prevent those things from happening. And I certainly thank you for your concern and information, but we do need to move on to another caller. I think we will take a couple more calls and then we are over time. But if the operator could give me the next call, that would be great.

Operator: Thank you. That will be Loralee Castner with the California Council of the Blind. Go ahead, please.

Loralee Castner: Hi. My question, my husband and I are both blind and are thinking of hiring someone to do some assisting for us, and part of that would include reading. And I wanted to ask how do you – what is the best way to request a background check?

Lisa Schifferle: Well, that is a very complicated question that can involve a long discussion of compliance with the Fair Credit Reporting Act in terms of requesting a background check. But in terms of getting them, there are a lot of sites like www.care.com that have background checks as part of their caregiver profiles, so you can choose caregivers who have already done a background check. You could also – I know when my grandmother was losing her vision she had hired readers to do a lot of her reading for her, but she, you know, saved any of her financial transaction type information for when I or my father came to visit so that we could help her with her banking. But the reader could help her, you know, read *The New York Times* and do the other things she needed to read along the way. So that is another option. But there are many online providers and caregivers that have background checks built into their screening mechanisms of the caregivers they provide.

Loralee Castner: Thank you.

Operator: Thank you. Our next question is from Debbie Pittman from the National Federation of the Blind. Go ahead, please.

Debbie Pittman: Thank you. I have two questions. The first one is, are there any accessible background checking agencies that can be utilized with screen reading software programs, that you are aware of? And my second question is, if someone is a victim of identity theft, can they get a new Social Security number?

Lisa Schifferle: Okay. I will start with your first question in terms of background checking and whether they can utilize screen readers. I do not know, but it sounds like there is a lot of interest in background checking and that might be a good followup Webinar for us to think about. This is our first foray into having a Webinar for the blind and visually impaired, so we are still learning about the issues ourselves and it sounds like background checking is a good one for us to look into more, and then we could provide more information about which background check companies might be able to be compatible with screen readers and give more indepth information about background checking caregivers.

Lisa Schifferle: In terms of the Social Security number and whether you can get a new Social Security number, it is extremely, extremely difficult, almost next to impossible to get a new Social Security number when you are a victim of ID theft. It can be possible in cases of domestic violence is one of the key exceptions to how difficult it is. But, otherwise, you are pretty much going to be most likely stuck with your Social Security number. And as Social Security points out, changing your Social Security number does not always solve the problem anyhow because oftentimes there are debts and other information that are associated with your name and other personal information, and not just your Social Security number. But you should not expect to be able to change your Social Security number, which is why it is so important to flag your Social Security number with Social Security and the IRS if it is compromised. Are there more questions on the line?

Operator: We just have one, and that is Michael [Laub?] with the Better Business Bureau. Go ahead, please.

Michael Laub: Yes, I was curious what persons might do if they have difficulty with the actual credit reporting agencies not correcting information?

Lisa Schifferle: Well, I mean first they can, as I mentioned, exercise their rights under the Fair Credit Reporting Act 605B or 611. If that does not work, our pro bono *Guide for Assisting ID Theft Victims* has a variety of followup letters that say, you know, "I have written you a letter under 605B and you have not followed my request to remove the information, and you are to by law," and further explains it. And that – those sample letters are all available in our pro bono guide at idtheft.gov/probono. But if those followup letters also fail, there are private rights of action under most provisions of the FCRA, and that is an option. People can seek legal help from their local legal services agency if they are income eligible, and legal services are usually for people at or below 180 to 200 percent of the poverty line, depending on the particular legal services agencies. Or, for seniors, regardless of income in many jurisdictions. And for people who do not qualify for legal services, the Identity Theft Resource Center is another resource that provides free legal help on identity theft related issues.

Michael Laub: I see now they are telling people to – the CFPB (Consumer Financial Protection Bureau) I guess is getting into the game of doing some of this with the credit reporting agencies, and I do not know if it is going to blur at some point what the FTC does and the CFPB or when folks might benefit from using that organization.

Lisa Schifferle: It is certainly worthwhile filing a complaint with the CFPB as well. Their complaints come into our complaint database, and they do have more resources devoted towards helping individuals. I mean if you file a complaint directly with the FTC, we do not provide individual assistance on each complaint, although it does, as I mentioned before, help generate an ID theft affidavit and also it helps us track trends and information, so it is important. But we would definitely encourage people to file complaints with the CFPB as well, and they have investigators who may be able to provide individual assistance on your case.

Lisa Schifferle: So I understand that was the last question, so we thank very much everybody for your time and for joining us in this Webinar, and we welcome your feedback and your suggestions for future Webinars that are targeted toward blind and visually impaired consumers and their advocates. Thank you very much.

Operator: Thank you. And, ladies and gentlemen, that does conclude our conference for today. Thank you for your participation and choosing AT&T Executive TeleConference. You may now disconnect.

[End.]