

Identity Theft: Resources to Help Clients Protect Their Identity – Live Webinar Captioning – 2.10.16

>>> Good afternoon, everyone Thank you for joining us today on our webinar on identity theft resources to help clients protect their identity. My name is Michael Roush and I'm the director of the real economic impact network at the national disability institute. Before we get started we have a few housekeeping tips to go over. I'd like to introduce my colleague Nakia Matthews who will go over these details. Nakia.

>> Thank you, Michael. Good afternoon, everyone. Michael, do we have the captioning slides in or should I just ad lib here?

>> I will take it back for just a minute. There is a slide out of order there. No problem. I would like to recognize our sponsor for today's webinar, which is Bank of America. Bank of America has been a long time supporter of the real economic impact network. Back to you, Nakia.

>> Great. The audio for today's webinar is being broadcast through your computer. Please make sure that your speakers are turned on and head phones plugged in. You can control the audio broadcast below. You can reopen it by going to the communicate menu at the top of the screen and choosing join audio broadcast. If you prefer to listen by phone dial the toll free number you see here and enter the meeting code. Please note that you do not need to enter an attendee ID. I'll leave this slide up for just a little bit longer in case someone needs to write down the numbers. Realtime captioning is provided during this WAEB webinar. They have been found in the media viewer panel. If you do not see the captions you may need to open the media viewer panel by selecting the media viewer button in the upper right corner of the webinar platform. If you'd like to make it larger you can do so by minimizing some of the other panels like chat or Q&A and conversely if you do not need or want to see the captions you can minimize that panel.

>> We will have time for questions at the end of the webinar. Please use the Q&A box to send any questions you have during the webinar to us and we will direct those questions. You can also use chat to send me Nakia Matthews or Michael Roush a question. If you are only listening and not on the web portion you can e-

mail Michael with questions at mroush@ndi-inc.org. Please note that this webinar is being recorded and that the materials will be placed on the NDI website at realeconomicimpact.org.

>> Finally, if you experience any technical difficulties please send the chat box to me, Nakia Matthews a message or e-mail me at nMatthews@ndi-inc.org. With that back over the Michael.

>> Thank you Nakia.

>>> For those of you new to the national disability institute I'd like to share information on our organization.

The national disability institute is a non-profit organization dedicating to building a better economic future for Americans with disabilities. We are the first national organization committed exclusively to champions economic empowerment, access development and financial stability for all persons across the full spectrum of disabilities. At the national institute we effect chain -- change through information, technical assistance and policy development to help the 1 in 3 Americans with disabilities living in poverty to take steps towards a brighter financial future. To learn more about the national institute go to realeconomicimpact.org.

>> We hope that if you are not already a member or a partnering organization of the real economic impact network we hope that you will join us for this national movement on building a better economic future for persons with disabilities. The real economic impact network is an alliance of organizations and individuals dedicated to advancing the economic empowerment of people with disabilities and consists of more than 4,500 members located throughout the United States. It includes a variety of organizations, non-profits, community tax coalitions, financial education initiatives, corporations and private sector businesses, federal, state, local governments and agencies as well as individuals and their families with disabilities. All partners joined forces to embrace, promote and pursue access to and the inclusion of people with disabilities in the economic mainstream. It's free to join. To learn more go to our website [realeconomicimpact](http://realeconomicimpact.org) on the organize. -- [realeconomicimpact](http://realeconomicimpact.org) on the organize. -- [real economicimpacteconomicimpact.org](http://realeconomicimpact.org).

>> This is definitely a topic that comes up from many of our partners from across the country on how do they help clients protect their identity but also what do we do if an individual we're working with has their identity compromised. An estimated 17.6 million individuals were victims of one or more incidents of identity theft in 2014. That's according to the department of justice. Persons with disabilities are not immune to this issue. At

times they may be more vulnerable to having their identity compromised. To share with us more information on this topic I'm grateful to have my new buddy, Cindy Lebis, the regional director of the southeast regional office of the federal trade commission share information with us on how we can help our clients but also what we need to know as well to protect our identity. With that I would like to turn it over to Cindy.

>> Cindy, you're good to go?

>> Yes.

>> I gave you the presenter so you can advance your own slides. Welcome Cindy. Thank you.

>> Perfect. Thank you as much -- thank you very much. I want to thank everybody who is on this call. I'm delighted to be doing this webinar today. I'm hoping that after this webinar you will come away with a lot of information not only about identity theft but a little bit more information about who the federal trade commission is and how we can help you in your mission and in your work and what you do. Let me tell you a little bit before we get started on identity theft about the federal trade commission. The FTC is a bipartisan federal agency with unique dual missions to protect consumers and promote competition. We are over 100 years old. We are an agency that champions the interest of American consumer. We're dedicating to advance consumer interest while encouraging competition in this dynamic economy. We have policy and research tools, we have hearings, workshops and conferences. We also collaborate -- we're a civil law enforcement agency and we collaborate with other agencies and other partners in industry and in law enforcement to further our curable mission. I'm the southeast director of the FTC. The FTC is a very small agency. There's a little over 1,000 employees. Most of the employees are in DC. We have eight regional offices across the country. About half of the employees in the agency do consumer protection work. That's what I do. My office does purely consumer protection work. Just to tell you a little bit about a few of the areas that we cover for those of you who have not previously worked with the FTC, we have a division of advertising practices. Our division of advertising practices does nationwide advertising. They look at ads on TV and print ads and ads on the computer and on the Internet. They look for whether the representations made in those ads if they're accurate, truthful and whether there's substantial claim in the ad. We look at dietary supplements, weight loss products, large national products that are advertised. A large variety. We have our division of financial practices and they deal with credit and financial issue across the board. We've

been very active in that area, especially with the economic downturn. We've seen a lot of problems in that area and a lot of missions dedicated to protecting consumers in the area whether it be lending or sometimes when folks are out there promising consumers they can save their homes for foreclosure, get them a reduced interest rate or even auto advertising. That's what our division of financial practices deals with. We also have a division of marketing practices. I call them our fraud division. They're the division in the FTC that deals with fraudulent solicitations that many of you may have gotten. Sometimes those robocalls you might get on the phone, folks promising you that they can save you from anything, get you something free, just all sorts of deceptive practices. That's what our marketing practices division does. Then we have our division of privacy and identity protection. That's the division that deals with privacy issues and identity theft. Now in the regional offices we deal with a little bit of everything and we bring law enforcement cases. We also do a lot of out reach. We work with groups like yours and we work with local organizations and my region covers seven southeastern states that works with all sorts of partners to do out reach programs to consumer groups, industry groups and all sorts of groups so that we can let people know we exist. I'm going to talk a little bit more in a bit about the different kinds of materials that we have to tell consumers to make sure they're protected against fraudulent practices and unfair practices.

>> Our federal trade commission act is a very, very broad statute. It protecting unfair and deceptive acts or practices. It's a very, very broad statute. It's through that statute that we bring most of our law enforcement actions against companies. Some examples of some of the cases that we've brought in this office are cases against deceptive debt collector, Microsoft scams where someone might call you on the phone and tell you they're with a large company and you have a virus on your computer and then you have to pay them to remove that virus, mortgage assistance relief cases where consumers are promising to save people's homes from foreclosure or somehow modify their loans. Just a variety of cases that my office handles. One of the things that we've done at the FTC is really focus on identity theft. In the past several years identity theft has been an area of concern. We have a data base called the consumer database. In this data base we've seen an up surge of consumer complaints whether they come directly to the FTC or in other agencies. An up surge in complaints over the past many years, probably 10 years in identity theft. Today we're going to talk about what is identity theft to start.

>> What is identity theft? Let's talk ability tax identity theft. Tax and benefits identity theft is very large. I'm going to talk about how does it happen, how can you reduce your chance of being a victim, what to do if you're a victim. Also I'm going to talk about imposter scams, whether they be IRS imposter scams or other imposter scams where people pretend to be someone from the government or someone from another agency when they're really not and all they are is out to get your money.

>> What is identity theft? The definition of identity theft is the misuse of another's personal information to fraudulently obtain goods and services, a job, medical treatment, medications, equipment, government services and benefits or it can even be to hide from government and law enforcement or others and using someone else's name pretending to be you. It's very broad. When I first started doing this what people thought about identity theft, they thought, well, it's when someone gets my credit card or when someone steals my wallet and they pretend to be Cindy. It's not necessarily that. It's anything that they may do to assume your identity and pretend to be you and get some sort of begin in your name.

>> Like Michael said earlier, the department of justice statistics show that just in 2014 there were 17.6 million, 17.6 million incidents of identity theft. In fact, that's 7% of the US population. That is an enormous, extraordinary number. As I often say to consumers, a lot of times we say, oh, my God the police needs to do something about this, somebody needs to do something. With that many cases of identity theft, that many victims that are out there it's very, very difficult for them to track down who are the perpetrators of identity theft, how they are getting that information and to prosecute them. While it may be disconcerting sometimes that means we as consumers have to do things to not only protect ourselves but to stop these thieves when they are perpetrating these frauds. The total number of identity theft complaints have increased. These numbers are based on the consumer database that I was talking about. The FTC has seen a rise of complaints. In 2013 it was about 290,000 and in 2014 it was 330,000. Just this last year in 2015 it's almost up to a half a million complaints that we have in our database. That doesn't include all of the (1) 700-0000 people -- 17 million people who have been the victim. Many times the people don't complain to the FTC. They complain to local law enforcement. Our database is an indicator of what is out there and how broad this problem is. This next slide shows identity theft complaints and the rise of those identity theft complaints

as reported to the FTC. What you can also see is this huge rise in what we call tax or wage identity theft complaints.

>> So back in 2013 tax and wage identity theft complaints were around 87,000. This year alone in 2015 -- or last year alone, 221,000 complaints. Almost 222,000 complaints about tax and wage identity theft. You know when I first started doing this 10 years ago and looking at the statistics we hardly ever saw this type of identity theft. It is increasing in the tax and wage area.

>> So the scope of this problem in the tax ID theft area is just really large. Again, starting in 2013 about 33% of all of the identity theft complaints pertained the taxes or wages. That was basically the same in 2014. This past year, 2015 almost half of all of the identity theft complaints in our database were about tax or wage identity theft. That's a huge change in the type of identity theft that we are seeing. A really huge change.

>> For last year January to December of 2015 this graphic shows how victims information was misused. Again, like I showed you before, government benefits is about half of all the identity theft. Credit card identity theft is now 16%. When I first started like I was saying earlier that made up the bulk of the identity theft. For some reason it seems that the identity thieves are focusing on taxes and other benefits that government agencies are giving to people or that people are getting in government agencies and other agencies. -- agencies. Some other areas are utilities, banks, employment, loans and then in general other types of identity theft.

>> What kind of government benefit fraud are we seeing? Like I said earlier, taxes and wage-related frauds are the bulk of the almost 50%. That would be a tax return that was returned in someone else's name. It could be some other wage-related fraud that people are getting, some other benefit. It can be any other kind of government benefit that's applied for or received or government documents that are issued in someone else's name, including driver's licenses that are issued in other people's names.

>> We've seen a huge, huge increase in imposter scams. I don't know if any of you out there have gotten those calls from someone claiming to be the IRS or somehow affiliated with the IRS or someone claims to be affiliated with a government agency and telling you that you have to give them money or give them access to your social security number or other identifying information because if you don't you're going to go to jail or the IRS will come get you. The surge in those numbers are almost 50 times as many as just two

short years ago. The FTC has actually been bringing cases against some of these imposter perpetrators. Often they're in other countries but sometimes they're here in the United States. Like I said earlier, for example, just a similar type of imposter scam that my office worked on was one of those tech support scams. A scam where the person said they were Microsoft or somehow affiliated with Microsoft or facebook but they could see that you had a virus on your computer. Sometimes they asked people to give them access to their computer, other times they just got your money and they claimed to be able to fix that virus on your computer. You know what, consumers had no virus on their computer or if they did they could not see it and they were not fixing that virus and they were just stealing millions and millions of dollars. They work not only from a location in Florida but also over seas in India. They took millions from American consumers.

>> What are some examples of misuse? I talked about it before. They may use your current credit card but they can also open a new credit card account in your name. That's problematic because you may not know for a very long time they opened a credit card account in your name. You may not know that they opened a new credit card account in your name unless you start then getting a debt collector call telling you that you might owe some creditor money for that Porsche that you didn't buy or whatever fancy thing the identity theft bought in your name or opened a line of credit in your name. You may not know it until you pull a copy of your credit report or go to get a loan for a car or mortgage and you find out that you cannot get that loan because someone else has a home in your name or ruined your credit. They can also open utility accounts in your name. They can even apply for employment or get medical care. In fact, opening utility accounts happened to my daughter. She got a call from a debt collector who said that she had an account with directv opened in her name. My daughter lives at home with me, she doesn't have directv and they had it in a different name but her social security number. Interestingly enough when we went to the police it was very frustrating because even though we knew the address where the account was set up the police didn't seem to be interested in finding the people and said, look, they're probably gone by now. That's why you are now the debt collector -- the debt collector is coming after you.

>> What is the impact on victims? Like I said before, denial of credit, denial of loans, denial of public benefits and medical care. You can lose your job. Especially people in the military. They have to keep their credit up

and they could have to explain or lose their jobs. Again, be harassed by debt collectors. If any of you has had to deal with debt collectors sometimes they can call repeatedly and bother you. Often people say, wait a minute that's not my debt and debt collectors don't believe people so they will hassle them over and over. We heard of people suffering severe legal cases and even being arrested. There was a story about someone in Atlanta driving around 285, our beltway, being arrested and they were on the TV crying saying it's not me. When you think about it probably every crook is saying officer, it's not me. In these cases it is a huge impact if you have to explain an arrest that's really not you for something that you did not buy or for a loan that you did not take out.

>> It causes stress and anxiety on people and the recovery time can be immeasurable.

>> A few years ago I was at a meeting about identity theft and there was a woman that was a victim of identity theft. She was telling all the different steps she had to take to try to make these problems stop occurring. She talks about having sent a complaint from FTC and she talked about talking to the credit bureau and they would take it off of her credit record and it was gone back on. She had a piece of paper on a small size legal pad and then she took them out and it not only went from her hands to the floor and she kept reading about all the things she had to do. Just when she thought it was over it would start again. Sometimes these identity thieves not only get your information but sell your information. You may not know where your information is and how it is being used.

>> If that's not bad, how does it happen? You think what happens. Well, some of the ways identity theft happens, it's not only tax identity theft but all kinds of identity theft. Lost or stolen wallet, Medicare cards. Often times Medicare cards have the social security number of the recipient on them. We have talked to agencies, we have talked to Congress people about can they change this. They've said it's a very, very expensive process but they are really taking into account that. Here in Georgia we used to have our social security numbers on our driver's licenses. That has thankfully since been changed. Also your smart phone has all sorts of information on it. If it's not locked and it is not -- and if it is easily accessible identity theft can easily occur. It can also occur by family, friends, visitors and advisers. You know, quite often we've heard that, you know, family or friends can use your information to obtain a lot of services. Sometimes it happens because, for example, a parent who has really bad credit can't get certain services, can't get utilities and

they might try to get it in a child's name. Or a friend or someone like a roommate might have access to information because you left that information out. We urge people to be very, very careful about leaving any personal identifiable information out for people to see. Dumpster diving. I used to see people route rooting around in a large dumpster and think how sad, maybe the person is homeless or hungry. Then I realized sometimes, no, that's not the case. Sometimes unfortunately the cases that they're rooted around the dumpster for, especially behind a doctor's office is to see what kind of information they can get. Stolen mail, which might include tax return information. Sometimes they get it through imposter scams. Remember I was telling you about the folks that call you up and tell you that you have some sort of problem with the government or you have some sort of problem with your computer. Often what they're trying to get from you is either you give them access to your computer, access to your information by giving them information they request access a lot of the numbers.

>> Corrupt insiders. Unfortunately we are only as safe as the folks that we give the information to. In tax returns we learned more and more about corrupt tax preparation services because they have access to a lot of information. We found that some tax preparers are taking the consumer's information and using it and getting money from the consumers tax returns.

>> How can it happen online? Data breaches. Boy, we hear about data breaches all the time. It seems like every day we hear about another data breach. I often wonder, I'm a federal government employee and I don't know how many of you are, but all of my information was breached. They have access to so much information about me. Some other ways it happens, phony e-mails from imposters. If you get an e-mail from somebody do not give them information. If you get an e-mail from somebody claiming to be your bank or your credit card company or claiming to be the IRS, you need to make sure that you do not respond to that e-mail. If you think, well, maybe my bank needs that information, maybe my credit card company needs that information for some reason, maybe they are telling me that I've had a breach and need my information, look on the back of that credit card, call the number for your bank that is the number that you generally call or go into the branch that you generally go to. Don't call the IRS number that they give you, call the number in the blue pages and the yellow pages or look up a number on your computer. Do not respond to phony e-mails.

>> Unsecured wifi is another place. If you're doing banking in a WiFi hot spot they can access your information that you are sending online in an unsecure WiFi hot spot. Never do any kind of banking or display any kind of personal information in a public WiFi hot spot.

>> Also peer to peer. File sharing and downloading software or APPs from unknown sources. Those are ways that people can get information. One of the other ways is sharing too much information online. It amazing me how much information people share online. You think, well, I'm not really sharing my social security number, but you share your name, you share your address. When it's your birthday on facebook that pops up. Now a crook has a lot of information about you. Sometimes all it is is as simple as them to Google information on you've to look at old records. A lot of the old records that the government agencies have on record contain your social security number and a lot of personally identifiable information. Don't share information unless you really have to or if you're going to share information you don't have to allow access to everybody and their brother.

>> What are some of the warning signs that you may be the victim of identity theft? Well, if your social security number is lost, stolen or compromised you may be the victim of identity theft. If you have an unusual delay in getting a refund you need to think, oh, I might be the victim of identity theft. IRS notification, they may send you a letter. They will not call you and they will not send you an e-mail to tell you. They will send you notification that there's been a duplicate tax return filing or some unreported income. For example, someone may have gotten a job in your name and now you have more income than you really earned or duplicate dependents that you don't have. That's a sign that something may be need and you need to contact the IRS.

>> What can you do to lessen your chances? Minimize your personal information. Minimize your personal information that you keep in your wallet or smart phone. I would say nobody needs to have a wallet that's 2 inches thick. You don't need to carry around every credit card that you got from some store where you got your 10% discount like you do and you opened up a credit card. You don't need to care reunion -- carry all those credit cards with you. You don't need to have information on your smart phone. Keep it lock in your office or home. Visitors that you may not suspect might be able to get that information. Keep it secure at work. Be careful what you share. This is what I talked about earlier. Don't give information unless you know

who it is, why they're asking, why do they need that information. I tell a story, my daughter was about 10 years old and she was in the girl scouts. You know, you're filling out the application for her to be a girl scout and it asks for her social security number and mine. I thought, why do they need my social security number or even hers? Thankfully I didn't know hers and I wasn't about to give them mine. I asked them, why do you need this. The person who I was filling out the information more said, I don't know. How many times do all of us go somewhere where we just routinely fill out that information? We routinely give our social security number to someone who doesn't need it. Theoretically some people who are asking do need it. Your bank probably needs it when you open an account. Your doctor's office needs it. What I tell people is they don't need it every time. Don't fill it out and wait until they ask you for it again. You know, the other thing is you don't necessarily -- if your Medicare card contains your full social security number don't carry it in your wallet or black out all of the numbers. You know what, if all the sudden you have to go to the hospital or need medical treatment your doctor probably already has that number from past visits. Or the hospital will treat you and you can get them the full information. If you're uncomfortable like some seniors are with that you can just leave the last four digits but you do not need to have the full number contained in your wallet. If you lose your wallet anybody has your social security number and a lot of other information that they can get from your license.

>> Don't click on links or unsolicited e-mails. Monitor and review all mail and financial statements. If you Macy's bill doesn't come don't think, yeah, I don't have to pay Macy's. You can call them and say I didn't get my bill, I just want to make sure it was sent and pay it. Review your mail-in financial statements to make sure that you're not getting, for example, debt collection notices on a bill that you don't owe or notices from the IRS or that your financial statements are accurate. Don't just get your credit card statements or your checking account statements and throw it in a pile. You have to look at it. Make sure there's not charges on your account or make sure you're not getting a bill from another credit card company that you didn't open or a loan for a car that you don't have. Really important, good, go to annualcreditreport.com. You can get a free credit record from each of the three major credit bureaus once each year. That means three credit reports. You can space them out over time and you can see if new accounts have been opened in your name. It's a great way to see that. You can see if there's a problem with some bills that are not your problem. It often

tells you a lot of information that's going on. It may not necessarily tell you that you've been the victim of tax ID or benefits ID theft but you should also put a copy of your credit report. I tell people when you're going online at annual credit report they will ask you a lot of information. It's scary when you think about how much information they have about you. It's a great way to monitor your credit.

>> Most importantly, dispose of information properly. If you are a business person you have some duties on how you have to dispose of information. If it's medical information or credit report information, you have duties on how you need to dispose of information that is your clients or people with whom you're doing business. If you're a consumer you also need to shred your documents or do as I do, rip it into little pieces and then throw it in the trash can and clean out my kitty litter boxes. Nobody is going through my trash.

>> For tax returns when you are preparing and filing tax returns and especially this time of year know your tax preparer. Know who you're doing business with. Don't just find a tax preparer on the side of the road. Really you need to know who is the tax preparer and what are their qualifications. Find out about them, ask your neighbors, ask your friends. It really is a problem that we've seen on the rise.

>> Mail your tax returns as early as possible in the tax season that way you won't be the recipient of the notice that says someone else has gotten to your tax returns before you and they have gotten your refund. If you're mailing don't put your tax return in out going mail and mail it directly from the post office. I say that holds true for really all mail. I suggest people don't put up the red arm on your post box at home. Do it at the post office because putting up that red arm is a signal to crooks out there that there may be something good in this mailbox.

>> If you're filing electronically as I talked about before use a secure network and store your returns securely and shred any drafts.

>> Additional advice for individuals with disabilities is protect Medicaid, Medicare cards that might contain your social security number. Protect personal information at home just like you would your cash or your jewelry. Make sure to open and review your mail and e-mail. Again, like I was talking about, if you get mail or e-mails from folks you don't know, don't respond to them directly. If you get some suspicious mail that says something might be wrong it might be wrong. If it doesn't make sense you need to look into it. Also ask medical and care facilities about their data protection policies. You need to ask them what they do. Do they

just throw out your information? They're not allowed to. You know, if you ever see someone throwing out that big long thing you just filled out you should get it and walk out.

>> Also, make sure to select assistance and other support professionals with care. It is very important to make sure you know who has access.

>> What to do if you're a victim. Whoops. Excuse me. Let me keep going.

>> What to do if someone stole your identity. There is a fantastic new website that the FTC has recently implemented. It is called [identitytheft.gov](https://www.identitytheft.gov). It is a really great resource for those who have been the victim of identity theft. It's a new website that is interactive and has just phenomenal information. On the new website you can report identity theft and get a recovery plan. It allows you to browse recovery steps to file a complaint, tell us what happened. You get a personalized recovery plan that is personalized to you. If you've been the victim of tax identity theft it's personalized for you and it's populated on what you tell us happened in the identity theft and then we tell you how to put your plan into action. What action steps need to be taken. It is just a really good user friendly site for victims of identity theft.

>> So when you click in you said what -- first you say what statement best describes your situation. You want to report identity theft, someone else filed a tax return in your name, your personal information was found in a data breach, someone got my personal information and wallet and I'm worried about identity theft or something else. You put in that information. Then we ask, what did the identity theft use your information for? Did they open up a credit card in your name, checking account, employment. What happened as a result of this identity theft. Then you will report the specific DLT details. This information will be reported to the FTC. It will also help you create an identity theft affidavit. The identity theft affidavit is essential because when you are the victim of identity theft you can contact the credit reporting agencies and get a 90-day fraud alert put on your credit fraud. orrode -- put on your corrode -- on your credit. In order to get a the that fraud alert, to have an extended fraud alert put on your account you need to provide the consumer reporting agencies with an identity theft affidavit and a police report so that you're showing them that this is a valid report of identity theft. Because of that the identity theft affidavit gives you all the information not only that you can use for the police but that you can use for let's say the credit card company or the business on

which someone opened an account in your name. This affidavit that's populated will give you what you need to further the process. It will also help you create your own recovery plan.

>> The affidavit is filled out. You will put in all of the information. We ask that you don't fill in the social security number or driver's license number but you'll fill in all of this other information. This can be used like I said to file a report with law enforcement agencies and to dispute with credit reporting agencies and creditors about identity theft problems. It gives all the information that they are going to need. Now your report isn't submitted yet. They have you create an account so that you can get a personal recovery plan. It has prefilled -- so it already has the letter and the forms for you. You'll be able to update, view your affidavit, change it. It will allow you to save so you don't have to keep putting in information over and over. Now, you don't to create an account but you can't make updates if you don't create a account. Then you get your own personal recovery plan. It tells you what to do. It may tell you talk to the bank or whatever. File a police report, fix your credit report. Each step in the process gives you more and more information.

>> Sorry. Let me go back.

>> It gives you more and more information. it will tell you why did they need this information, what else it needs and how it can be used by folks. It puts a complaint into the FTC database. Why is that important? Those numbers I showed you earlier on are used not only to track the number of identity theft complaints but can help law enforcement agencies see trends and problems in a certain area. So, for example, if all the sudden we are seeing a lot of surge in identity theft complaints coming out of one particular area we will work with law enforcement. Law enforcement has access to the data federal 24/7 where they can see these trends and maybe do something about some of these identity theft complaints and maybe target some of the folks that are perpetrating these identity thefts.

>> It's 10 minutes before we're going to stop so I want to open this up to questions. I've gone on and on. I'm hoping there's some questions out there that hopefully I'll be able to answer them for you.

>> Great. Thank you so much, Cindy. Thank you for all of this great information. We do have several questions. Hopefully we'll be able to get through all of them. If you have a additional questions go on and keep putting them in the chat box, in the Q&A box and then we will direct those questions. Before we get into the questions though I do want to share a personal example of how this information particularly during

tax time is really important for us to be aware of. So I'm a vita volunteer. I provide free tax preparations services through VITA services. 2 years ago we were doing taxes for a group home that -- actually, there was a few at the group home all owned by the same group. As we were doing the taxes for individuals we noticed that their tax returns were being denied. Come to find out somebody else had already been filing their taxes for several of the individuals in the group home but the individuals were not getting the tax returns or they had no record of doing it. So in that situation because we were doing their tax return being denied we were able to identify that their identity had been stolen and be able to rectify that situation. I just share that as an example because of the work that we do in this field there's multiple opportunities we might hear or witness these situations and where we can be advocates. Now we have additional tools to share. I just wanted to be able to share that example of how we were able to identify several individuals whose identity had been stolen during tax time.

>> That's wonderful. If you're -- one thing I didn't say is if you're identity is stolen or if you are the victim of tax ID theft you definitely need to also contact the IRS. They have been really great at advocating for victims of identity theft. They have on their website information. They will provide victims of identity theft with a special pin number that will be used to file a tax return that will make it more secure when you file in the future.

>> Great. Okay. So we're going to see how many questions we can get through. So we're going to do kind of a speed round. All right.

>> So the first question that's coming up is, if an individual signs up for the do not call list how long does it take to get off the number? How long does it take for their number to get off the list?

>> You mean how long does it take where you don't get those calls anymore?

>> Yeah.

>> It should stop within 30 days. Now, let me make a lot of caveats on do not call. On do not call your name -- or number may still be called by political organizations and those of you who live in some of the states where the primaries are early you're probably getting those calls. Charities can still call you. If you tell them to stop calling you, that you do not want to receive those calls they must stop. Within 30 days companies who are telemarketing to you must stop. They have to take you off the list or take your off their call list.

>> So it's a follow-up question to that. What if I am on the do not call list and I get calls from the groups that are calling to say I'm with the computer company and want to check the security on your computer and they still contact you? If I didn't -- to the person who asked that, if I didn't say it right please submit it in the chat box.

>> That's a great question. Let me tell you, that's the problem. The folks that are perpetrating the frauds do not care about the do not call list. They don't care if you're not on the do not call list. Many of them are in other countries. They are calling and they don't go by the list or check against the list. That is a good indicator that they're probably a fraudulent operator. You may still be getting those robocalls telling you they can cut your credit card interest rate deduction or get you an auto warranty or all sorts of calls that I still get. Unfortunately many of those calls while we bring law enforcement actions as do state attorney general's offices and US attorney's offices and all sorts of law enforcement agencies we work together to try to stop these. We actually at the FTC had a thing called a robocall challenge. We are trying to -- we had a monetary challenge for \$50,000 to come up with a product or a process to stop these robocalls. Often they come from phone numbers that seem to be an number in your area code or really they're coming from other countries or they're spoofed phone numbers. We are working to stop it. We are bringing law enforcement action. The best advice I can give you a hang up or just don't answer calls that you don't know. Often times if you don't pick up the phone and don't answer that's the best way to handle it. I agree with you, it is something that is frustrating not only to us but many, many law enforcement agencies.

>> Great. Thank you. For the next question for corroderedit reports how can you tell if you might have -- be a victim of identity theft?

>> So, for example, you might see an account that is not yours. Now, it could just be a mistake. Let's say there's an account on mine and it's an American Express account that I never opened and it's got a lot of activity that I can see and it looks like from that account I haven't made my bills in 6 months. That would show me that it's a mistake and I can contact the credit reporting agency. They make it very easy to let them know that there's a potential mistake or that I might be the victim of identity theft. Then they come back and will ask you a lot of questions. That may indicate that you're the victim of identity theft. With my daughter, for example, she was able to see it with a debt collection letter, that it was an account. When we called the

company they said we have our social security number. They read me the last four digits and they were hers. You just can see another account that might be open or you can see one of your accounts that you haven't used in years is being used now.

>> Great. All right. So it's 3:56. We're going to try to get two more questions quick in here and then we'll close up.

>> Is it free to do the fraud alert?

>> Yes. One other option in addition to a fraud alert you can put a credit freeze on your credit account. You can freeze your credit. That means you won't be able to get credit, nobody will be able to get credit in your name but then you have to unfreeze it. From what I understand, it's very easy to unfreeze but it may not allow you to make a impulse decision in 5 minutes or in 15 minutes. It can take sometimes hours or days even I've heard of. I've actually heard from several people it can be in an instant. That's something to think about. It's something to think about with children. There's been a rise in child identity theft. Sometimes you can put a freeze on you're child's account if there is one.

>> Great.

>> We're going to get one more in here. That question is, whether the new chips on the credit cards help protect our identity?

>> You know, I understand that that chip is supposed to make it harder for an identity thief to use your information. I apologize, just really don't know how they work and how it is supposed to protect you but my understanding is that's the way of the future. That's what they're all using now. I think it may hopefully cut it down but that would cut down the credit card kinds, not necessarily the tax and benefits type.

>> Great.

>> Lets Mohamed Emwazi make -- let me make one final pitch because we have a minute left. If you have questions go to the identitytheft.gov remember site. For anybody who wants to do their own webinar or give a presentation to a church or synagogue group or a group of friends we have information that can be used by everyone to get this information out. We have brochures that are free and they are fabulous. We have all sorts of information because we are a tiny agency but we want this information out to everybody. If you want information on how to do that go to the FTC's website. If you have questions please feel free to call me. I'm

accessible. Not that I can help you necessarily solve your identity theft probably but probably point you in the right direction.

>> Great. Thank you so much, Cindy. We will be following up because we could not get through to the information today to do a follow-up webinar potentially on the scams we receive regarding work from home opportunities. Be on the look out. Be on the look out for that. We will potentially be doing that webinar later on this year. If you're interested in that please be sure to send me an e-mail just so we can be sure to make sure you're included on that. If you're not part of the real economic impact network I hope that you will join the network. You can go to our website and do that. I would also like to share information on the American dream employment net work. You can go to Americandreamem.org to learn more. This is a new program at the national disability institute to help innovative program to support the employment of individuals with disabilities. Please join us on March 9th for our next webinar on empowering prosperity, integrating into human services. We have a friend that will be providing that information to us. I would like to thank Cindy for the information today from the federal trade commission. This is great information. I'd like to thank any colleague, Nakia Matthews, as well as all of the other staff members that are a part of the NCI assistance training program. We look forward to connecting with you-all next month on March 9th. Thank you so much to -- thank you so much for participating on today's webinar. Have a great afternoon.

>> Thank you.

>> [Event concluded]