Please stand by for realtime captions.

>>
>>> Welcome to the FDLP Webinar, IdentityTheft.gov: Your one-stop resource to help people recover from identity theft . My name is Jaime Hays. I will host a webinar and we also have Laura Flint doing technical support. The presenter isCarol Kando-Pineda who is a project manager for outreach to public libraries at the Federal Trade Commission. She is the Council and the Federal Trade Commission's division of consumer and business education and leads teams to create and distribute free online articles, social media content, printed publications and videos to help people spot scams and manage money. She had at the military consumer initiative and outreach to consumers. She began her career as a staff attorney bringing false advertising cases. She became the agency's legislative counsel serving for several years as a liaison between the FTC and Congress. In 2014, she worked in a consumer issues -- on a consumer issue and she earned her degrees. I will walk you through some of our normal housekeeping reminders. If you have questions, please feel free to use the chat box in the bottom right-hand corner of the screen and I will keep track of questions that come in and at the end of the presentation, we will respond to each of them. We are recording the session and will email a link to the recording and slides to every register. We will also be sending you a certificate of participation using the email you used to register. If anyone needs additional certificates because multiple people are watching with you today, please email us and include the title of the webinar along with the names and email addresses of those needing certificates. If you need to zoom in on the slides, you can click on the full screen button in the bottom left side of your screen. To exit, mouse over the blue bar at the top of your screen so it expands and click on the blue return button to get back to the default view. At the end we will share webinar satisfaction survey with you. We will let you know when the survey is available and the URL will appear in the chat box and we would appreciate your feedback after this session. Including comments on the presentation style and value of the webinar. I will hand the microphone over to Carol Kando-Pineda.
>> I appreciate you sharing your time with us this afternoon. I think you will get some helpful tips on identity theft that are useful for patrons but really useful for anyone. Very often we have to use them for ourselves. Including friends, colleagues, a neighborhood association, house of worship, sometimes it's helpful to share the information with those you know that might be going through some sort of an identity theft problem.
>> I am speaking for myself and not on behalf of the Federal Trade Commission. All of my remarks are my own. We will cover identity theft and various forms of identity theft and talk about what to do if you suspect you have become a victim of identity theft or you are concerned about information being compromised and also a data breach.
>> Let me throw this out there to get you thinking about this. What type of identity theft is on the rise? Child, tax, credit card, medical? Think about it silently or you can put an answer on the chat box and we can look at them and see what people are saying. I will give you a second for that. These are not the only forms of identity theft. It can strike any of your financial accounts or files. I selected these because they are the ones you hear about the most. Somebody has said, medical. All of them. We are getting a sampling of everything. It is credit card identity theft. The reason that the surprise is that this kind of where identity theft started 15-20 years ago when FTC was first charged with monitoring identity theft and gathering information about the way it was happening and the effect on victims and his staff trends. Identity theft is where it started. Over the last four or five years we have seen a rise in tax identity theft, so that was steadily on the rise. Almost at alarming rates and really skyrocketing for a couple of years. Now we are seeing it start to decline a little bit. It's down by 46% compared to what it was last year. It's a big drop but that doesn't mean the identity thieves have gone away. They have refocused on credit card identity theft because that is up by 23%. That's an interesting statistic because it shows you the fluid nature of this crime that scammers will do whatever works for a while and when it stops working,

either because we are warning people and people are getting the knack on how to avoid them or it's just not probable, they morph into something else. Maybe just switch tactics or try a different kind of identity theft. This by no means will stay this way permanently. We don't know. It could easily change in flip-flop or be something else but that is the state of identity theft right now. What is identity theft? We think of it in the classic way as somebody stealing your credit card account information and opening new credit cards in your name. It can be much more. Somebody can steal various bits of your personal information and open utility accounts, apply for tax refunds, they can get a loan, apply for a job and maybe even get medical care. You can imagine the impact on victims. You may be denied credit or loans or public benefits or you might not be able to get your tax refund. Somebody may use up your medical benefits and you won't be able to get medical care based on your medical benefits. You might be harassed by debt collectors pursuing the debt as if it were yours because it looks like it was opened up in your name with your information. In the extreme, you may see legal issues like if there is an arrest warrant out for you under your name because of something that a criminal did using your name and your Social Security number or personal information, you could be arrested for something that thief did. That's a very extreme example but it does happen.
>> For the victim, there is stress, anxiety, recovery time, expenses. It is always been the burden falling on the victim to prove who they are and what happened and there's a lot of paperwork and a trail that is created for that. That can be a big burden for people.
>> How does identity theft happen? It's not always online hacks. That certainly does happen. Sometimes it happens in the regular old-fashioned way. Somebody loses their wallet or purse or it's stolen. Dumpster diving. These will get into a dumpster and see what kind of papers they can find. Medical receipts, prescription bottles etc. They might not need to find all of your information in one spot. They might already have some and try to match it up or mix-and-match. Very often and get into the thief might be able to acquire personal information from a corrupt insider whether it be at a bank, hotel, car rental, medical clinic. Any place where there's going to be personal information. Somebody might be able to compromise it, take it and resell it. Online it happens with things like fishing emails -- phishing emails. They used to be easier to detect and would be formatted incorrectly or something off about a logo and easier to spot the language. They are much better. You can't judge a necessarily a phishing email just based on the appearance of it. You really have to sort of have your skeptic hat on and do a little research before you respond to anything that looks like a bank or some sort of an account reaching out to you looking for personal information. Legitimate companies aren't going to call you or email you and ask you to send all kinds of login information and passwords or Social Security or any kind of sensitive personal information. They would find other ways to manage that account with you. It's always wise to stop and take a breath before you respond to anything like that. Data breaches are a big source of compromised information. Credit card scamming. I took a picture we have about skimming. You see the hand removing part of an ATM machine to reveal the arrow showing where the skimming device has been placed so that as soon as you put your credit card, debit card in, they can read all of the electronic information and they have stolen your information. They can be quite good and are hidden. You often can tell something has been tampered with and never looks obvious that something has been tampered with, don't use it it may be reported to the financial institution. Let's go on to the details of credit card identity theft. This graphic expresses the surprise that people tended to have when they realize it's on the rise again. There's other forms of identity theft that were becoming much more prevalent and we are back to warning people about the regular credit card identity theft. If you suspect use been a victim of credit card identity theft, standard identity theft, generally there will be a warning sign. You might get a statement in the mail or statement in your online account with charges that you don't recognize. There may be a statement from a credit card or utility account or some other account that you know you didn't open. You know it doesn't belong to you and all of a sudden you're getting a statement. Those are warning signs. You may have told your credit report to look at a transaction or perhaps you are

buying a house and need to pull your report. You may notice charges that don't belong to you or accounts that aren't yours. That's your first tipoff there is identity theft . Call the companies where you know the fraud occurred. In some cases, that's simple and in other cases it may be more complicated. There may be other companies to call. It depends on your individual situation and how long it has gone on for.
>> On the back of your statement is a customer service number or a fraud line. Call the fraud line and tell them that there's been an account that was opened in your name and it's not yours or theirs unauthorized charges on my account and I want them taken off. That should take care of that. You will probably have to go back to them once you get verification and paperwork done to confirm and verify but we will get to that.
>> Place a fraud alert on your credit report file. The three major credit reporting companies Equifax, Experian, Trans Union maintain credit files on anybody that uses credits, which is probably 90% of us. That credit file comes from the different accounts you might have and all of the different retailers and merchants you do business with, utility company. Everything else. That consists of your file. The report is a snapshot in time. When you call to get your report or you go online and get your report, it shows the snapshot taken at that particular time. It shows all of the activity on the report, just to clarify. Once you realize identity theft maybe a foot, -- afoot, you want to contact the companies and order a credit report as an identity victim. That shuts down access to your account so that anybody looking to grant you credit has to jump three through more hoops to verify identity. Hopefully that will prevent identity theft from spreading. You want to get your credit report so you can examine them all carefully. They are a snapshot and pull from a lot of the same sources so they will be very similar but they may not be identical. They may pull slightly different information or focus on one thing more than another. One may be more up to date one may lag a little bit but it's the snapshot. You want to go through those carefully and see if there's mistakes, unauthorized charges, account you don't recognize that you didn't open and you want to mark that up and formally send that back with a letter to the credit reporting companies and tell them these are not my charges or my accounts and this is a mistake and please correct my credit report.
>> If that doesn't work, there's other mechanisms. You can learn about those on IdentityTheft.gov . You can use those to enforce your rights and make sure that information comes off. For a lot of people, the fraud alert is enough and getting the credit report, marking it up and asking them to clean it up for you.
>> Here is a question. Does anybody know how long a fraud alert lasts? You may not know at all or you may have an idea in your head. For many years, you credit alert was good for nine months and you could renew it. Now, it's a trick question because there was a new law that passed last year that went into effect in September and fraud alert last an entire year. Rather than 90 days they last for a year. That's a nice benefit for identity theft victims. You can renew can renew it every 90 days, but you would have to renew it 3-4 times over the course of the year but if you wanted to have it in place. Especially if you needed to do groundwork to prove you are the identity theft victim . You can get an extended alert for seven years but that took more work. If you have the fraud alert in place for a year gives you time if we had to start renewing things and you might be able to go to the extended alert or just lift it depending on how complicated the situation was. Another aspect of the new law was that credit freezes are free for everyone. A credit freeze is kind of the step up from the fraud alert. My credit freeze completely locks down your credit. Nobody can grant credit in your name. You can certainly lift it if you needed to get credit and place the freeze again. There is usually a cost involved in it depended by state. Whatever state you lived in is determining the cost to lift and to place credit freezes. They are free for everyone throughout the country now. It doesn't matter what your state law says. That's going to encourage more people to consider that as a possible option. If you are in the market for a home or you are getting a student loan or perhaps an auto loan, you might not want to freeze your credit immediately. You might want to take care of that transaction and once that is done, freeze your credit.

Sometimes I do a lot of work with the military community and sometimes if there is somebody deploying and their spouses left behind, they want to take care of a lot of that before they put alert on the credit report so that the spouse left behind has got everything they need while the other spouse is deployed. It depends on your situation where the want to go the fraud alert route or the credit freeze route. It's good to have that. You can also freeze your children's credit if they are under 16. You could do it for incapacitated adults, as well, which makes managing affairs easier. Starting next May, the same law provided for free credit monitoring for active duty military -- I believe the genesis of that is that once servicemembers are deployed it's more difficult for them to check credit and to do a lot of those transactions. Sometimes the online systems aren't always compatible overseas. Sometimes the phone lines are only staffed according to U.S. times and it depends on where you are in the world so you might not be off-duty when the call line center is open. A lot of servicemembers were sending in handwritten letters to order credit reports. The free credit monitoring helps them maintain things and keeps track of files. It's a nice benefit for our servicemembers and military family.
>> Just a little bit more about the fraud alerts because it is an important consideration. To get there for alert under the new law you only need to contact one of the credit reporting agencies or companies. They have to contact the other two. It requires creditors to take an extra step to verify your identity. The extended fraud alerts for victims of identity theft -- you have to do a little bit more but that last seven years. You can get that with an identity theft report and I can show you how you can get that. Before the credit freezes you have to contact each of the CRA's and that's one consideration people may keep in mind. They just want to go for the quick, easy, simple but not a complete lockdown, the fraud alert is a good option. If you want to lock it down and you are willing to contact all three, the credit freeze is for you. You can do it online or by phone. Under the new law the credit reporting companies have to place your freeze no later than one business day after the request if you have called or done it online which is another improvement for consumers. If you want to lift it, it has to be lifted within the hour. That takes some of the sting without completely locking down the in freezing credits because you can lift it relatively easily and place it back again if you need to conduct business and get your credit. By mail, they have three business days. That's still a pretty reasonable amount of time.
>> You can also get a credit freeze under the law referred to as "protected consumers." If you care for elderly relatives or have guardianship, conservatorship, have a child with a disability, another relative that can't manage their own affairs, that will help you a lot. You will have to provide proof you have the authority to do that with a court order or guardianship or conservatorship paperwork, fully executed power of attorney. You will probably also need to show proof of the person's ID and proof of your ID, drivers licenses, some sort of government approved card.
>> We have been through the first two steps. Let's talk about the final step. Reporting the identity theft to the FTC by going to IdentityTheft.gov. That's the one stop shop for identity theft recovery. I will walk through that in more detail soon and give you those details. The most important thing about reporting to the FTC, aside from the fact that this is how we keep track of trends and how identity theft is evolving and what consumer victims needs are it helps the identity theft victim generate a recovery plan that is personalized to their situation. They can get sample forms and letters online. They will get a printed complaint and they can save it as an identity theft report and in a prior statute, it's a legally defined instrument. It's a way you can exercise a lot of your rights as an identity theft victim allow you to prove that you are the victim. It's a very helpful tool for the victim to have to start that recovery process.
>> Let's talk about these special forms of identity theft them we will get to IdentityTheft.gov. That's my reminder that most of the time, people realize that they are a victim of tax identity theft because they file their taxes and expect their refund and they get a note that says, somebody has already gotten the refund and file taxes under the Social Security number and you are not entitled to them and you are thinking, what just happened? You might get a notice in the mail if the IRS sees a discrepancy if you and the thief file at the same time but a lot of the time you file your taxes and they tell you that refund is

gone. Tax identity theft happens when somebody takes a fraudulent tax return using somebody else's Social Security number and can earn wages using a Social Security number and it might even try to claim somebody else's children as dependents or try to file a tax refund for a deceased tax payers information. If people find something is up with her tax refund and the suspect tax identity theft, they should complete the IRS identity theft affidavit form and this is the number: 14039. You can get it at that link and also at IdentityTheft.gov. You can fill that form out and submitted through IdentityTheft.gov to the FTC and they will pass it to the IRS so they have it and it eliminates a step for the consumer. After you file the form, file your refund, pay your taxes and IRS should be in touch and keep you up to date on what's happening and make sure your file is clear or if it's been flagged. If that doesn't resolve your situation, this is the number for the unit at IRS that you would call. 1-800-908-4490. We can put that in the chat box toward the end of the presentation. That is the unit at the IRS to call if completing the affidavit does not rectify your identity theft situation. Place a fraud alert on your credit report to make sure there is no further damage. If you suspect it has crept into other parts of your financial accounts, order the credit reports and look at them and send them back corrected to get that rectify.
>> Medical identity theft. Another graphic to illustrate this. It is what you would expect with fraudulent use of a Social Security number, Protected Health Information. The thief would use that to get a medical treatment, exam, prescription or two fortunately health insurance or Medicare.
>> This is not as widespread as credit card identity theft. I have an interesting statistic that said that 2.3 million Americans have been affected by medical identity theft. Probably not as large as the 17 million estimated identity theft victims identified in the U.S. but that's the best we have. Supposedly that's up from 1.8 million just a few years ago. Definitely something to watch. If an identity thief tries to sell a Social Security number on the black market they can get $1. If they sell a medical identification number, health insurance, or medical account, they can get $50 on the black market. $1 for a Social Security number and $50 for medical information. You can see it can easily become more of a problem because the fees can make money -- fees -- thieves can make a lot of money. Get your medical records from your healthcare providers. You may have to pay for them and sometimes it's expensive. I wouldn't go immediately. If you notice something on your explanation of benefits or statement that doesn't seem right, I don't think you have to order all medical records for the past 10 years from every doctor or clinic or hospital that you have been at. You probably want to take a more surgical, no pun intended, approach and start exactly at the hospital, clinic, doctor's office where you know there was an issue, and get your records. Look over them and get the records for a year maybe or several months surrounding we think the incident happened. You can backtrack and see if they went to other places or they got other services or prescriptions were things like that. Order the record accordingly. You will have to correct each one. Not only will you be really expensive but time-consuming and frustrating to have to go through thousands of pages of medical records if you start off with everything. You want to build up your file and look at everything and go from there. Send the corrected record back to health care provider and tell them that these records are wrong and you want to get them corrected.
>> You do have rights under state law with medical identity theft. It depends on the state. You may have to do research to figure that out. Let's talk about child identity theft. Here is a poor little baby. Kids don't have credit reports. In most places, under a certain age, nobody will extend credit to you. You are not legally entitled to get credit. Kids under 16 probably should not have a credit report. If you find out they have one, that's a sign of trouble. What percentage of identity theft complaints to the FTC are from people 19 or younger?
>> This is kind of a trick question. It's 5%, so not quite the highest but 5% is still pretty decent for any particular demographic. There is an ID analytics study that says children were seven times more likely to experience this kind of fraud over adults, which is kind of interesting. Social Security misuse was 51 times higher than that of adults. I don't know if those numbers are still true because they are probably about seven years old at this point.

>> It's still an issue and you should be aware of for the young people in your life. Kids in foster care have a harder time with identity theft. That's a more documented problem. Kids in foster care will tend to live in several different places and information is being shared probably many more times than a child that's living with their family. Just the fact that information is being shared back and forth, there may not be somebody to advocate for that child. At least not in terms of identity theft or credit information. Probably making it more likely that people will try to take advantage and sometimes it's a family member that steals a child's information. It may be hard to correct because the child may know they stole information because they needed to get utilities or needed a credit card to survive, so the child doesn't really want to get a family member in trouble so they won't report it. That leaves the child with ruined credit. It's a tough problem. If you find that there is fraud committed using your child's Social Security number, use the same things he would do if your number was misused. Contact the company, utility, whoever and asked them to close the account. Because kids don't usually have those credit files, contact each of the credit reporting companies and asked for a manual search for your child's Social Security number. Each one has a different process. You will have to reach out to them through the fraud department to find out what you need to do to get that search done. You can request a freeze for free and do it easily and that maybe well worth doing to keep the credit frozen before they reach a certain age. If you've got children anywhere from 7-14, 15 you might want to request that manual search to double check. At least by the time they are 15 or 16, that is when they are probably starting to think about getting a car loan, student loan, maybe graduating and going to work, applying for jobs. We want to make sure their record is clean and there is no credit report or charges that somebody else made before then to give you time to get that cleaned up by the time they need to do that. We have a booklet on child identity theft and I will tell you how you can get that in a minute.
>> We talked about the different forms of identity theft. Let me show you IdentityTheft.gov. It is run by the Federal Trade Commission. To get started and file a complaint, click Get Started. The big benefit of identity theft.gov is you can get a personal recovery plan. If you put in all the information indicating child identity theft, you will get the checklist that tells you what to do for a child identity theft. If it's tax ID theft, you will get a check list to reflect the things to do for that. It gives you step-by-step advice and what you need to do giving you tips on how to do it. If it says you need to send a letter to the credit reporting company, once you put your information in, you can generate the letter to the credit reporting company. We have sample letters that will auto populate with your information so you can print that out and have your letter to the credit reporting company ready to go. When you print a complaint and you fill it in, it becomes an identity theft report and you attach it to the letter. That is one step taken care of. That will hopefully move it ahead on recovery. There is the IRS form that you can file. You can find it on the site, fill it in and submitted to IdentityTheft.gov and we will share it with the IRS. There is a chat and phone support along with a Spanish-language site. It's always free and it's secure.
>> This walks you through the steps of filing that complains. I wanted to give you a sense of what it looks like. If you think your credit card accounts were compromised, check that off. It will walk you through what you need to do to get your specific details and how you can create that identity theft report and get your recovery plan. This is what the identity theft report looks like. This is what you get after the process. Right before you submit, it asks you to open an account and it's free. You can do all of this without opening an account if you don't want to. The benefit is that as you learn more about the situation -- let's say it was tax identity theft and resolved within a couple of months and all of a sudden you see unauthorized charges on your credit card and now you've got a different problem to address, if you have an account, you can update it and get a new identity theft report to send to the new round of people and to show the history of the problem. You can still go back and file a new complaint and get a new identity theft report but you have to start from scratch. If you have the account, all of it is saved and you can update it.

>> This is what your recovery plan would look like. It tells you to call the Bank of America, place the fraud alert. You can go back in and check and it will prompt you. If you didn't tell them that you heard from Bank of America and this is what happens, it will prompt you as a reminder. It tells you to put in the date so you can create your paper trail and file to keep track of it. You might be able to resolve identity theft immediately but it could pop up again he might have some paperwork again, so is good to have that trail.
>> This is what one of the sample letters look like. It has the FTC IdentityTheft.gov at the top, so that's an indication to people that you filed a report with the FTC. This is how you check off what you've done. This is another sample letter. It populated with the information in that situation. This is the IRS form. Let's talk about some of the things the average person can do to stave off identity theft. The number one thing I would tell people aside from protecting information and being careful that you shared with, you want to monitor your accounts. Get in the habit of checking your statements and accounts. Whether it's a paper account or you go online, pick a time and a place convenient for you and do it on a regular basis. You don't want to go for too along. Even if there is an account for you haven't bought anything and there is no charges, just make a habit of taking a look and checking to be sure nobody else is using it and is no charges on it. When your mail comes in, open immediately. Don't let it sit for a couple of weeks and open everything, if you can help it. There may be mail that yours showing an unauthorized charge or you may be getting a statement from an account that's not yours. If you wait a few weeks, give them a few more weeks's time to run up charges before you step in and correct it. If you know you are getting a statement in the mail, you want to know when that comes in and be on the lookout. If it goes missing or it's not posted when it is supposed to post or you don't get the mail, that's a sign of trouble. Also helpful is to get in the habit every year of ordering your free credit report. We all have the right to an annual credit report from each of the credit reporting companies. If you stagger your requests, you can get them all at once if you want to and that's fine. They calendar to do it at the first of the year or whenever they change the batteries in a smoke detector or in June. Link it to something meaningful so you remember to do it. What would be good about staggering is that, the credit report is a snapshot at any given moment. If you see one version in February and maybe it's fine and another in June, if there is a problem, you have gotten to it six months earlier than if you had waited until February to get all three together. You are seeing a version of your credit report every few months helping you to spot a problem. This is on IdentityTheft.gov. This is the contact information for the credit bureaus for fraud alerts, credit freezes and opt outs and a good cheat sheet to have because it has a lot of the good information.
>> We've got a booklet about recovering from identity theft and avoiding it. It's a little booklet. If you are active in any type of civic associations, in your neighborhood, friends and colleagues, it is helpful to hand out to make available to give people you know the basics of what they need to know about identity theft.
>> Another site you know about is FTC.gov/bulkorder. You can usually order as many as you need. Sometimes there's limits on what's available due to inventory and print budget. If you really need to have 800 copies of something for an event, you can order more and there is contact information and you can write to somebody and ask for more for an event and we will do the best we can to accommodate you.
>> If you want to use any content on the website or print publications, you are free to do that and they are free in the public domain. We love to hear about it because if somebody is giving stuff out at the library, that magnifies the effect we can have. We love to know about it but you don't need our permission to do it but we love when you share the information with us. This is a snapshot of materials. We have eight photo pamphlets on issues affecting Spanish speaking people. We have a booklet for older consumers. There's a lot of different interesting stuff. Feel free to look around and order things you think might be useful. We've got a blog you can subscribe to. Go to FTC.gov/subscribe to subscribe.

If you find it's not working for you, go back to FTC.gov/subscribe and you can take your name off the list. I think I've given you a really quick overview of identity theft and possible strategies for recovery and some good resources. Along with ways to get FTC information. I'm happy to answer any questions. Let me look at the chat box to see what people said.
>> Other than a fraud appearing on an insurance statement, how would you know medical information was compromised,
>> It might be an explanation of benefits at the end of the year and you might see on the list of things something you don't recognize aside from a statement. You might go to your doctor and they may say, you've used up your benefits for this particular thing for that year and that would be a sign somebody else has been using them. It's usually a statement or explanation of benefits.
>> What's troubling is that aside from using up your benefits, which is serious enough, if somebody else is getting medical treatment using information their medical records are mingled with yours. Your doctor may be looking at misleading information when trying to determine what treatment to give you if somebody came in with a different or related element.
>> When is it too late to report things are fraudulent credit charges to the FTC and other agencies?
>> It's never too late to report it and try to get things resolved through the usual channels. In terms of being able to get the refund on your credit card, there's certain timelines by law where they have to take charges off and investigate and get back to you and you have to provide information once the timeline is triggered. It's always in your best interest to report it as quickly as you can. Even if you think you may have missed a deadline, I was to report it because if it was a result of identity theft, there may have been no other way to know those charges happened.
>> If you are told to info was compromised, are there additional steps to take?
>> Our programs like LifeLock worth while?
>> I can't endorse any particular product. You can do research on the FTC site and learn about an action we brought against LifeLock. There's things monitoring companies can do for you. You want to know what you are paying for and what you are getting out of it. If somebody offers you free credit monitoring you should probably take it in the event of a compromise. A lot of that you can do yourself but if it's free and from a company that compromised your information, you may as well take it and make it easier on yourself. It's a convenient way to monitor your credit.
>> If you are told to info was compromised, are there additional steps to take?
>> info was compromised, are there additional steps to take?
>> It depends on your comfort level and your particular situation. Some people will freeze credit because there's been so many data breaches just to have that added level of security and peace of mind and now that it's free, there is no hardship involved. Not everybody wants to take that option or do that. That is a possibility if you wanted to do something extra.
>> I used to think URLs were safe but is there some agency keeping people from using http websites?
>> I do not now.
>> What are your top three preventative measures consumers should take to prevent credit card theft. Monitoring statements protects it after it appears.
>> One of my top tip is to get the annual credit report and monitor it closely. Sometimes you don't know until something happens. Sometimes a thief may ping your account with small charges to see if you notice and if you don't notice, they may put $10,000 on it. I still and it's helpful because if you get in the habit of monitoring statements, credit reports, knowing when things are due, and staying on top of that moving financial picture, as soon as one thing doesn't seem right, you will be able to act on it. It may not rise to the level of a full on identity theft. They may not put more charges if you get a corrected and you are on top of it fast. The other top tip would be to be careful with how you handle your personal information and who you give out to. Shred paper documents. Be skeptical when you get pop-ups, phone calls, emails from somebody that claims to be a company you do business with, the government.

This may not sound like it's related to identity theft but imposter fraud is probably the biggest complaint that we have gotten in the past year. It takes many different forms and can be somebody planning to be a relative that is stuck in a foreign country and the phone line is garbled and you can hear them but it's sounding like your cousin and they need money to be wired to them right away. Not only can you lose money but they can open you up to identity theft if you start to share information with people that you think you trust and you know. Those situations people should be aware of. If somebody is pressuring you to wire money or send them pin numbers on a gift card to take care of your taxes or get you relative out of trouble, different kinds of situations. That's a hard red flag if you are pressured to pay them immediately, send them money, wire the money or send them a gift card it's probably a scam.
>> Do you have a list of steps of what to do if you are a victim of ransomware?
>> I don't know that we have a list of steps but we have an article about ransomware. The tough thing about that is -- it's what to do before hand. Backup files regularly. It's not just a matter of file hygiene and you have it just in case you need it. There is no ransom to be had if you have a backup to all your files because you can just re-create files and put them where they need to be. That's probably the best tip I have.
>> On December 4, we have Train, Maybe for the Olympics. December 6, managing someone else's money. This is the link for the satisfaction survey. We would appreciate if you filled out the satisfaction survey at GPO. Thank you for presenting a wonderful webinar and thank you for tuning in to FDLP Academy. We will forward -- we look forward to seeing you at future webinars.
>> [Event Concluded]