Jean Fullerton (00:00):

Today, we're going to discuss elder financial fraud. This is a growing problem where someone tries to take advantage of an older person for financial gain. This webinar is geared towards older adults themselves, but also friends and family members who want to be able to recognize the dangers and reduce the risks of fraud. My name is Jean Fullerton and I'm a Certified Financial Planner with Milestone Financial Planning. You're welcome to enter questions during the presentation and we will try to get to all of them at the end of the presentation.

Jean Fullerton (00:35):

So let me tell you what we're not going to cover. We're not going to cover what to do once you get into trouble. We'd rather talk about what to do to prevent getting into trouble. And we're not going to talk about the advice you always hear about complex passwords and shredding your documents, you know all that. We'll try and give you very specific actions to avoid fraud and theft and scammers. So let's get started.

Jean Fullerton (01:10):

So older adults tend to be more of a target because they actually have financial resources, retirement accounts, and they often own their own home. They tend to be more vulnerable because they're often isolated or living alone, and without nearby family. Seniors also tend to be more trusting and they can be dependent upon others. In fact, sometimes they're dependent upon their victimizer. In some cases, they may be cognitively impaired as a result of dementia or cognitive decline. They may also be embarrassed to admit their situation or reluctant to turn in their abuser.

Jean Fullerton (01:51):

Older adults are also less familiar with technology and social media. However, this turns out to often be an advantage. Younger people are more often victims than seniors, because younger people share more information about themselves on social media that can be used by thieves to steal a person's identity. You're safer if you don't share information such as your birthplace, your date of birth and say your vacation plans on social media.

Jean Fullerton (02:25):

There are many different types of fraud. Today, we're going to talk about fraud that involves the misuse of credit cards, bank accounts, and personal information. Scams can take many forms. Oftentimes, they're carried out using postal mail, computer interaction or your telephone.

Jean Fullerton (02:47):

Let's start with mail fraud. You may receive a letter in the mail congratulating you for having won a prize or the lottery, or that you've received an unexpected inheritance. These letters almost always fraudulent. The scammer makes money by asking you to pay a small fee or taxes on the amount in order to receive your windfall. You may even receive a check in the mail. Signing the back of the check may actually result in your unknowingly signing a contract. Or if you deposit that check into your bank account, you may be subject to fees or penalties when the check bounces.

Jean Fullerton (03:27):

Another common mail fraud scheme involves a fake charity asking you for money to help out victims of the latest disaster, such as a hurricane or even a fire at a neighbor's home. These schemes are very compelling since most people are receptive to an appeal of this sort. Another different type of scam is a letter informing you that you have a lost financial account that the sender can recover for you for a finder's fee.

Jean Fullerton (04:00):

So the way to avoid this type of mail fraud is number one, you should know that any prize from a non-US entity is illegal so you should never respond to a message of that sort. You should never send money to collect on any prize or lottery winning. Never sign or deposit an unexpected check and be wary of requests from unfamiliar charities. You can check out the status of an official charity at the website charitynavigator.org. And you can also go to the charity's website directly to find out more information about them.

Jean Fullerton (04:44):

For the situation where someone claims that they can recover a lost account, you may actually have an old account or credit with a financial institution that has been turned over to the state as abandoned property. In this case, if you actually do have a lost account, you can find the account yourself without having to pay a finder's fee by going to the website, missingmoney.com.

Jean Fullerton (05:15):

Another form of financial fraud is computer fraud. Computer fraud has become a very common problem. Thieves can send out millions of email messages with very little chance of getting caught. If even a very small fraction of recipients fall for their message, their effort can be very lucrative. A common technique is referred to as a phishing scam. The bait in this case of phishing is that the email message appears to be from an official source, such as your banker or a well-known company.

Jean Fullerton (05:55):

The thief's intention is to have you click on a link or a file included in that email to either gather personal information from you or to install a virus or malware on your computer. For example, you may get an email that appears to be from your bank that warns you that your account will be deactivated unless you click on a link to upgrade security. In this case, that link within the email would take you to what appears to be your bank's website where you would enter your credentials, but it's actually a fake site that is stealing your information to be able to access your bank account.

Jean Fullerton (06:41):

Another example is a message from what appears to be say Microsoft telling you that there's been an unusual sign-in activity that you need to respond to. Another form of computer fraud is referred to as spoofing. In this case, the email appears to be from one of your friends or contacts, but that email address is fake, or it could actually be from the email account of your friend if your friend's email account has been hacked, and that email is actually coming from the thief.

Jean Fullerton (07:20):

Here is a sample of a phishing scam email. The bait in this email that looks like it comes from a well-known company PayPal that is asking you to confirm your login credentials. This is a much more

sophisticated scam than the old Nigerian prince with bad grammar scam. The red flags in this case are the sense of urgency, a threat to freeze your account, and a note that you can't reply to this email account.

Jean Fullerton (07:56):

So in order to avoid being a victim of computer fraud, the most important way is to never click on anything in an email message without thinking. If you're concerned about a message in an email, you should go directly to the website that that email appears to be from rather than clicking on the link in the email. Also, if you move your mouse cursor over the link in the email, you should be able to see the address that you would be sent to. If it doesn't match the link text, or if there is no translation, that's a dangerous link.

Jean Fullerton (08:39):

If the text of the email from your friend doesn't sound like them, beware it may be a spoofed message or your friend's email may have been hacked. Also, beware of a popup claiming that your computer has been infected. This is a common scam. It's always best to keep the software on your computer and your phone updated with the latest version to take advantage of whatever security upgrades have been put in the software.

Jean Fullerton (09:13):

Here's an example of a fraudulent email. In this case, we see a message purported to be from UPS and they want you to link on the connection to verify delivery. But if you hover your mouse cursor over that link, you will see that it goes to some other location rather than what the link says. This is a big red flag and simply delete that message.

Jean Fullerton (09:47):

So let's talk about phone fraud now. Phone fraud is becoming more and more common. There are also red flags for a phone fraud to look out for when you get a phone call. Fraudulent phone calls usually have some sense of urgency, intimidation, threats, or just repeated calls. The intention is to get you to react without thinking first. For example, you may receive a phone call that appears to be from the police, the IRS, or maybe from a local court telling you that you've done something wrong, such as not shown up for jury duty and that you need to pay a fine, or that you need to confirm some personal information.

Jean Fullerton (10:34):

In some cases, it's simply telemarketers that are using high pressure tactics and sometimes frightening calls in order to sell you something. Fraudulent calls can be sophisticated by faking the phone number so that they appear to be from the official source or in some cases to be from somewhere in your neighborhood. One of the worst scams is a fake distress call from what sounds like one of your young relatives who is in trouble and needs money. They may claim to have been arrested and asked for bail money. There's often a request to, "Please don't tell mom."

Jean Fullerton (11:15):

So in order to avoid phone fraud, you need to know that government officials never contact you by phone or email. So if that's who it appears to be from, you can be sure that it is fake. Whenever you

recognize a red flag, slow down and understand that this is likely to be fraudulent. If you're concerned about the message, simply hang up and contact the agency directly. Also, never call back a one ring phone call. That's another scam that will add a fee onto your phone bill.

Jean Fullerton (11:57):

In fact, it's safer to simply not answer phone calls from phone numbers you don't recognize. If appropriate, the caller can simply leave you voicemail. Never give out any personal financial or medical information over the phone, unless you have initiated the call. If you get a distress call from a relative, contact the family to confirm the situation. Use your mobile phone option to block callers. You can block phone calls from valid marketers by adding your name to the website donotcall.gov.

Jean Fullerton (12:37):

You can reduce the amount of mail and email for marketers by adding your name to the DMAchoice.org website. And it's a good idea to add your name to the OptOutPrescreen.com website to decline offers for credit and insurance. This prevents the credit agencies from selling your information to financial institutions.

Jean Fullerton (13:10):

So let's switch to Medicare fraud now. Medical insurance fraud has become more of an issue than identity theft for many people and it's more lucrative for the thief. You can actually buy someone's personal information on the dark web for about $25, but to buy medical insurance information costs more like $2,000, because the payoff is potentially much larger. With fraudulent uses of your Medicare insurance information, it can be very difficult to undo the damage. When you go to use your insurance, you may be denied coverage for either services or medical equipment.

Jean Fullerton (13:52):

The fraud can even change your medical records, including diagnoses or blood type for example. You could even receive the wrong treatment or harmful treatment because of misinformation in your record. One way of committing medical fraud is to offer someone free services, such as DNA testing or cancer screening with the assurance that the service would be paid by Medicare. The goal is to get you to turn over your Medicare information, which they can then use fraudulently.

Jean Fullerton (14:27):

The warning signs of medical insurance fraud are bills for services that you never received, notification of a limit of coverage, denial for a condition you actually don't have, and receiving unexpected medical supplies. You should protect your medical insurance cards the same way you do your social security card. Don't keep them in your wallet unless you're actually going to a medical appointment. Shred all your documents and prescription labels that have Medicare information on them. Review all your Medicare statements for accuracy when you receive them and decline free equipment or services where they want your Medicare information.

Jean Fullerton (15:19):

So there are other areas of fraud that you need to look out for. Reverse mortgages and Veterans Affairs benefits are two areas of concern for senior citizens. Reverse mortgages are used to be able to benefit from the value of your home while still being able to live in your home. These financial products are so

often misunderstood or misused that you must receive help from a government approved financial counselor before you're allowed to arrange for a reverse mortgage.

Jean Fullerton (15:56):

In a similar fashion, individuals who help senior citizens with Veterans Affairs benefits must be accredited before they're allowed to give advice. When you need services at home, avoid contractors who approach you. You should look for service providers who are recommended by other members of your community. You should check for licenses, insurance and any outstanding complaints.

Jean Fullerton (16:23):

One very effective way of avoiding credit fraud is to put a credit freeze on your account so that no one can open up a line of credit or a credit card in your name. In order to do this, you must contact all three credit agencies. Because of a new federal law, putting a freeze on your credit is now free of charge. Please note, however that if you want to open up a new credit card yourself, you'll have to first unfreeze your credit record.

Jean Fullerton (16:58):

So here are some additional actions you can take. You can sign up for a free service called Nixle. This is a service that provides notifications from your local police department about timely warning, such as severe weather and traffic alerts, but also about current scams. Go to nixle.com for text messages on your phone or email messages.

Jean Fullerton (17:25):

You should remove any automatic overdraft protection on your bank accounts. This sounds like a convenience, but eliminating it will limit your exposure to theft. If your bank account is compromised, this way you prevent an attempted theft that exceeds the value of your account and you're notified of the attempt. You should provide your bank and investment institutions with a list of trusted contacts that they can contact if they can't get ahold of you.

Jean Fullerton (18:00):

There are also new laws that allow your financial institutions to block any suspicious withdrawals. Here is an example of a Nixle alert from a local police department that warns residents, that there have been reported phone scams where the caller ID appears to be from the local police department. And the caller is warning the victim that they need to clear up an arrest warrant by paying a $3500 fine. So this is an example of how Nixle can help out.

Jean Fullerton (18:47):

So there are some actions you can take on behalf of an older person. You can set up a daily check-in call service. Oftentimes this is a free service offered by your local police department that automates a daily call. If the call is unanswered multiple times, they will contact you. There are also paid services available, such as CareCheckers and IAmFine websites.

Jean Fullerton (19:17):

One of the best things you can do is to set up an automatic email notification whenever their credit card is used. Oftentimes, you can even get notified of the amount of the charge and the location where the

card was used, so you get immediate notification if someone is using the card fraudulently. It helps to set up an automatic payment of debts, such as utility bills and receipts of income, such as pension benefits so that there are no checks received or sent in the mail.

Jean Fullerton (19:57):

You can also set up a third party notification on long-term care insurance policies so that you're notified if the premiums are not paid and the policy is at risk of termination. And a good idea is to have the older adult tell a trusted contact where to find important documents, passwords, and keys.

Jean Fullerton (20:24):

So in terms of suggestions for good advice for people of all ages, don't allow websites to remember your credit card information. You've heard of all the security breaches of well-known companies. So it's worth the time to read type the information in the future to protect from the company losing your credit card information to a hacker. Don't reuse passwords, use unique passwords for every website. Use a password manager to remember all those different passwords and create strong passwords.

Jean Fullerton (21:04):

A password manager securely keeps track of all your passwords, and you only have to remember one master password. Don't access financial accounts on public wifi networks. That free wifi and Starbucks may be compromised and someone could be reading your information as you're typing it.

Jean Fullerton (21:30):

If you're concerned about an older adult, here's some signs to watch out for. If there are unpaid bills, large bank withdrawals, or unusual credit card activity if you notice something missing valuables or the house not being cared for, or if the older person themselves is not cared for properly. If there are changes in personality or if the older person is isolated, or if someone new speaks on behalf of the older person. If there are new or unusual friends or new names on financial accounts, and of most concern is if there are unexpected changes to estate documents such as a will or a beneficiary designation.

Jean Fullerton (22:23):

Here are some actions you can take. If you see signs of financial abuse, you can report fraud to the Adult Protective Services in your state or elderjustice.gov. Or if you believe someone is in danger or there has been a crime, then you should contact your local police.

Jean Fullerton (22:45):

For mail fraud, you can report abuse to the US Postal Inspection Service. For computer and phone fraud. The appropriate government agency is the Federal Trade Commission or the FBI Internal Crime Center. For someone who's the victim of financial fraud by an individual, you should definitely contact the local police.

Jean Fullerton (23:13):

Here are some more resources that you can use to learn more about elder fraud, how to avoid it and how to deal with it if and when it happens. So that wraps up our webinar for today. So we will open it up for questions.

Jonathan Harrington (23:32):

Thanks, Jean. We do have a couple of questions. The first is password managers and aggregators. I know you had mentioned those during the presentation that you found those useful. Do you have a particular recommendation on which one to use?

Jean Fullerton (23:49):

So there are a few password managers. There's usually a small annual charge to use them, although they often have free trial periods. A couple of the larger ones that we liked are LastPass, L-A-S-T-P-A-S-S and a second one is 1Password, the digit one, P-A-S-S-W-O-R-D.

Jonathan Harrington (24:24):

Great, thank you. Next question. If you find that you have something on Missing Money website, how do you claim it? Is that an easy process?

Jean Fullerton (24:37):

It turns out it is a very easy process. So when you go to Missing Money, you can simply type in your name and it will show you a screen such as the one I have up here, I entered the name Margaret Bennett. And what it does is it shows you all the abandoned accounts in the various states for a person named Margaret Bennett, regardless of the middle initial.

Jean Fullerton (25:10):

And if you see a name that matches yours and you perhaps recognize the address and/or the financial institution that has turned over your account, you can simply click on the claim button and enter your information. And that claim will go to the local state and they will get in touch with you to claim that account.

Jonathan Harrington (25:39):

Great. Thank you, Jean. The next question has to do with powers of attorney. Do you recommend using powers of attorney to help elderly parents prevent financial fraud?

Jean Fullerton (25:50):

Ah, that's an excellent and somewhat complex question. So in general, we recommend that everyone have a financial power of attorney so that someone can step in if they are incapacitated. And this is particularly true for older adults and for single older adults, it's very important.

Jean Fullerton (26:16):

However, you should note that this is only relevant if the person is incapacitated. The person still retains the ability to manage their own finances and that means that they can be the subject of fraud. What we might suggest in addition to the power of attorney is to have the person put you on their account as an agent or to give you duplicate statements so that you can recognize when something unusual happens in their account.

Jonathan Harrington (26:59):

Okay, thank you. Another question here about age groups. Are any particular age groups targeted by financial fraudsters?

Jean Fullerton (27:13):

The group that is targeted most are people who have been the victims of fraud in the past. So if this has happened to you, you need to be especially vigilant in the future. As I said earlier in the presentation, it's actually younger people that share more information that are most at risk of becoming victims of identity theft in particular.

Jean Fullerton (27:43):

However, people over the age of 65 are particularly vulnerable because they have Medicare insurance, which can be very important for fraudsters who are looking to get a free $20,000 surgery done. So it affects all ages in different forms.

Jonathan Harrington (28:12):

Okay. Another question related to checking in on parents. Do you think that parents, elderly parents would be turned off by their children trying to help them with these types of topics?

Jean Fullerton (28:31):

In some cases, absolutely. So this is a very sensitive subject and you have to recognize that older people can be very independent and not want to be dependent or to share sensitive information with family members. So there are various techniques you can use such as the call in, does not ask for any financial information, but it keeps people in touch, which seniors usually appreciate.

Jean Fullerton (29:10):

And that way you can kind of keep tabs on what their situation is. In other cases, you might recommend that the senior engage the services of a financial advisor and perhaps share information with the non-family member advisor, which can help to keep tabs on someone.

Jonathan Harrington (29:42):

Great. Well, I think that is the end of the questions. We appreciate everyone joining the webinar today. As we mentioned at the beginning, we're sending the recorded version of this out to all participants and it will be posted onto our website. And we will be sending out information on our next webinar, which will be in November. Thank you for attending and enjoy the rest of your day.