Elder Abuse & Travel Vulnerabilities: Fraudsters Never Take a Vacation
August 2021

Lyman Clayborn:
Good morning, everyone. Hello, I am Lyman Clayborn. I am the coordinator of services for older adults at Brooklyn Public Library, and I am here with my colleagues at the library. I would like to mention Judith Vigo, who is here as my programming coordinator and co-host of this event. Welcome to Elder Abuse & Travel Vulnerabilities: Fraudsters Never Take a Vacation. This is a perfect time for this program. Everyone that joins this program is on mute and please stay on mute until speakers ask for questions and then be sure to unmute yourself to ask the question. And then, obviously, please mute yourself back when it's time to stop your question. You may put questions into the chat that Judy and I will monitor throughout the program. And we will have a Q&A section for this great presentation. This program will be recorded live. Anyone who does not wish for their image or voice to be shared as part of our broadcast, please turn off your camera and your microphone at this time. Additionally, please be aware that your name may appear in your zoom window. So, if you want to change that, you might. For the past six years, Brooklyn Public Library has been proud to partner with Apple bank, being rooted in the greater New York area for over 150 years. Apple Bank strives to improve the quality of life in the neighborhoods it serves through community involvement and personalized financial services. Apple Bank sponsors a wonderful array of Brooklyn Public Library programs and services, annually, including multi-lingual family programs and beloved programs for older adults like our Creative Aging series. Today, Apple Bank and their partners at the US Postal Inspection Service are joining us to talk about how to help educate and protect members of our community from travel vulnerabilities and mail scams. It's my pleasure to turn the program over to Danielle Blakely, Senior Fraud Investigator at Apple Bank, Thank you, Danielle.

Danielle Blakely:
Thank you, Lyman. Good morning everyone. As Lyman stated, my name is Danielle Blakely, and welcome to today's virtual seminar. Before we get started, I would like to ask Jim Matera, Apple Bank's Chief Retail Banking Officer to say a few introductory remarks. Take it away, Jim.

Jim Matera:
Thank you, Danielle. Welcome everybody to this seminar. This is something that is really important to the participants but also to Apple Bank. We've been in these communities in Brooklyn, Apple's been around for over 160 years. And when it comes to elder abuse and mail fraud, Danielle and Kristen who on the call can tell you more about this than me, but this is an ongoing problem that we see, for our customers and for the Bank. Literally daily, we see claims come in, especially from mail-based types of fraud that really trouble us. We do our best to help our customers not suffer any losses from that but it is really something that people need to be very tuned into and I know that this seminar is going to provide some helpful hints, tips and advice on how you might be able to avoid becoming a victim of this type of fraud. We're really committed to helping our customers and helping new people really take care of yourself financially. So, with that, I like to hear what the group does have to say. This is the first one of

these I participated in, but I also want to just lastly thank the library for its partnership. We have been partners now I think for maybe more than five years in a number of areas. This is a great way for Apple Bank and the library to really touch the community and provide some services and advice to go well beyond what we think that a library and a bank should be doing to the community. Thanks, Danielle, I will give it back to you.

Danielle Blakely:
Great, thank you so much, Jim. So right now I will share my screen. Sorry. So, this presentation will be on Elder Abuse & Travel Vulnerabilities: Fraudsters Never Take a Vacation. And, like Lyman and Jim said this is the perfect time to speak about this being summer and upcoming holidays and travel for all. So what is elder financial exploitation? Elder financial exploitation can be defined as the fraudulent, illegal, unauthorized or improper act that uses the resources of an elderly, excuse me, elder for monetary or personal benefit, or that results in depriving an elder of rightful access to or use of benefits, resources, belonging, or assets. Elder financial abuse can take many forms, including scams by telemarketers, forgery, identity theft or the use of undue influence to pressure an older adult to transfer his or her assets under false pretenses. Close to 90% of elder financial abuse takes place in domestic settings, rather than long-term care facilities and is normally caused by family members. This can be done through promises of lifelong care or through the use of power of attorney, authorizing the fraudster to access the elder's financial assets. Given their age and possible dependence on others, coupled with the fact that older adults tend to have more financial assets, the elderly are particularly vulnerable to financial exploitation. Especially the case where elder financial, excuse me, an elderly individual and they have suffered from some mental ailment that weakens the ability to make sound financial decisions. The impact of elder financial abuse. As senior financial scams are a multibillion-dollar industry studies estimate that annual financial loss nationwide to be around $2.9 billion. Consequences include financial loss, mental health issues such as depression or anxiety and/or physical complications from counterfeit drug scams. Due to the embarrassment, retribution and fear of loss of independence, instances go unreported. In fact, only 1 in 44 incidents of elder financial abuse is reported to authorities. Many questions may arise, in that event. Who's going to take care of me if they reported the behavior? Will my caretaker be angry? If I report the abuse, will it be investigated? And, will my abuser be told that I have reported this issue? If I report the abuser, will they still be responsible for my care? And will I be subject to worse treatment in the future? Education and awareness are two key strategies for preventing and responding to elder financial abuse. 10 scams that cost older Americans the most money in 2019. The figures below are from the 2019 Federal Trade Commission provided through the FTC commission Sentinel Network, an online database on frauds and other consumer-related harm. So, number one is romance scams with $83.7 million. Number two, government imposter scams which are $61 million. Prizes and sweepstakes and lottery scams at $51.4 million. Business imposters for $34.3. Investments at $24, excuse me, $25.4 million. Computer tech scams are $24.1 million. Timeshare sales at $17.4 million. Family/friends imposter scams at $17.1 million. Online shopping for $14.2 and timeshare resale scams at $12.5 million. Fraud impacts various age groups. Nearly six times, excuse me, fraud impacts, various age groups differently. The FTC says consumers who are 60 or older are nearly six times more likely to report losing money to computer tech scams, three times more likely to report losses from prizes/sweepstake/lottery scams, and two times more likely to report losses from family and friend imposter fraud. Some warning signs to look out for. There are many warning signs of elder financial abuse, but not one single thing is definitive proof. Below are some warning signs to be mindful of. Number one is unpaid bills which the elderly should have the means to pay. Purchasing or spending

behavior that appears to be out of character. New best friends, which are people who have recently become close to the elder who is not promoting the elder's best interest or claiming the right to funds. Sudden changes in financials, which could be drastic drops in funds or drastic increase of funds from unknown sources. This could also be changes in an elder's will, trust, insurance or other financial documents. Abrupt or unexplained transfer of assets. And lastly, confusion about recent financial arrangements or changes. Tips for prevention. While there are many different scenarios of elder financial abuse, here are some steps to take now, before a crisis may develop. Have a trusted discussion about finances. It was found that those who discuss finances with a trusted family member, friend or financial professional felt better educated and equipped to prevent elder financial abuse. Exercise caution when providing your financial or other personal information over the phone or internet and resist the pressure to provide unknown sources financial information or access to your financial accounts. And always ask for more information in writing and get a second opinion before changing your power of attorney, wills, trust or your personal financial information. There are three banking moves to consider prior to traveling. While most of us are eager to travel again, setting up your finances before traveling requires some time and attention. One, contact your credit card company. Notifying your credit card company before any trip can help ensure the institution will not freeze your cards while you travel due to suspicious activity, or assist to catch fraud. Notify your bank. Banks can also freeze your debit card/checking account if there is frequent suspicious withdrawals in a foreign country. Informing banks where you are traveling to and when you will be away can also help them catch unauthorized and suspicious transaction. Carry some cash. Carrying physical currency with you is predominantly safer than paying with cards, both in terms of staying within budget and reducing the risk of identity theft if you end up visiting a less than legitimate business. Vacations and holidays are a time to focus on desires outside of work. Whether it's sightseeing, visiting a family member or a break from your nine to five grind, the last thing you would want to worry about when you're away is your financials and something happening to them while you're away. While these three steps are not as fun as actually planning your vacation, spending a few minutes outside to this, to schedule, trying to tie these loose ends can make the trip more enjoyable. Dangers of posting travel plans on social media. Over the past few years, it seems the standard part of many people's vacation is snapping a photo and posting it to social media as soon as they arrive. However, posting pictures and checking in on social media while away could potentially leave your home vulnerable to thieves. The best time to post-holiday pictures is when you are back at home. I actually just got back from vacation and a lot of my friends were wondering why I haven't posted social media until I got back. And it was mainly due to the fact that I did not want to stress about someone seeing me gone, and wanted to ensure that once I was home and safe and all of my finances were in order, that's when I posted. They got to enjoy it when I was two days back in the United States. Posting updates that place you far away also gives thieves ample time to plan and execute a robbery at your house. Never assume your post is only going to your friends, even if your privacy settings only allow friends to view your posts. Your friend might be reading your update at a coffee shop, anywhere, unaware that a stranger is viewing over their shoulder or they could be logged in at a computer outside of their house and they leave it open for someone to see it afterward. Ways to protect yourself while traveling. Here are some tips to ensure you will not return to any unpleasant surprises. Clear out your mailboxes, number one. Mailbox theft is completely on the rise and we will get to that in detail in the later part of this presentation. Mail piling up is a tip off that no one is home. Have a trusted neighbor, friend, or house sitter collect your mail and packages and keep them safely out of sight. Notify your financial institutions. Add a travel notice to your debit card or credit card to make sure

you have access to your money when it is needed. Keeping receipts from purchases you make in unusual locations is a preventative measure that can help financial institutions catch fraud on your account. And number three, checking accounts regularly. Get in the habit of checking financial accounts before you leave the hotel and when you return. The sooner you spot unfamiliar or fraudulent behavior, the better. Oh, please note, it is best done on your personal device, and not a shared hotel device. Also, please be mindful about using unsecured Wi-Fi. Number four, sign up for eStatements. Protecting your information from being stolen or delivered to the wrong address. eStatements are secured by your online login credentials that you create yourself, ensuring your statements can only be accessed by you. Please be advised that although the statements themselves may not provide a full window for the fraudsters, they may be able to piece together enough information, including information from other sources that they may have obtained to attempt identity theft. Switching to ACH payments for bills. No form of payment is completely foolproof; however, data indicates that paper checks are the payment method, most affected by fraud. Benefits of eStatements. They reduce mailbox clutter, eliminating the bulking of envelopes to a dozen times each year will lighten your load when you start to sort through a pile of mail to sort out what is important. Faster delivery because eStatements do not require you to print and prepare mailing and spend time traveling in the back of a mail truck. You will usually see your statements several days earlier than those sent with a physical paper statement. Email notices when your statement is ready to view, print or download. Once your statement is ready to be accessed or is available online, an email will be sent to you, letting you know you have access. Easy access and retrieval. Manage your statements the way you want. You can simply go online whenever it's convenient for you. Enhanced security. By viewing your statement online you can eliminate the chance of someone stealing your statement out of the mailbox. Automatic storage for your records. Excuse me. It's super quick to find, and once you examine your accounts, just select the monthly statement that you would like to view, and it's right there available for you. Environmental benefits. By choosing to go paperless you are saving trees, reducing chemical munitions and you're lowering your carbon footprint. For additional information, please visit www.applebank.com. The CFPB and FDIC released an enhanced version of Money Smart for older adults. On July 14, 2021, the Consumer Financial Protection Bureau and the Federal Deposit Insurance Corporation announced the joint release of an enhanced version of the award-winning financial education curriculum, Money Smart for older adults. The Money Smart for older adults program was developed in March 2019 by the Federal Deposit Insurance Corporation and the Fed, the Bureau of Consumer Financial Protection to raise awareness among older adults and their caregivers on how to prevent elder financial exploitation. It encourages advanced planning and informed financial decision-making. This enhanced version includes a new section to help people avoid romance scams, which is obviously on the rise, as well as an updated resource guide. Romance scams commonly occur when a scammer creates a fake profile on a dating site or app and strikes a relationship with a target and then seeks money. Money Smart for older adults is a free curriculum that includes an instructor guide with presentation content speaker tips, hands-on activities, presentation slides and a resource guide for participants. We have listed the download below, which is available for everybody as well. DOJ has a new elder fraud hotline. The US Department of Justice launched a new elder fraud hotline in March 2020, which offers free help to people aged 60 and older who may have been victims of financial fraud. It is created by the Department's Office for Victims of Crime. Staffers trained in elder abuse answer questions about romance scams, contractor fraud, computer tech support cons, fake Publisher’s Clearinghouse sweepstakes, among others. The hotline may be reached by calling toll-free 833 Fraud 11 and is staffed seven days a week from 6 am to 11 pm. Fighting fraud. There are numerous

ways that you can limit the sales and scam calls that people get daily, multiple times a day. You can get on the National Do Not Call Registry. To register, visit www.DoNotCall.gov, or call 1-888-382-1222. You can also use Caller ID and screen calls, block telemarketing and robocalls, and remember the phone is a one-way street. So, if you do not answer, they have no answer from you. And below, if you or someone you love is experiencing elder abuse, please call one of the organizations listed below this will be available for everybody's view after the call, after the seminar. Please see the information below. These are helpful resources and information about elder financial abuse. Please visit the list below. That is it on my end. I will now turn this over and stop sharing my screen. This will go now go to postal with John and Donna.

Donna Harris:
Thank you, Danielle. Can you continue your screen sharing?

Danielle Blakely:
I'm sorry, yes.

Donna Harris:
Well, while she's sharing her screen, I'm Donna Harris. I'm the Public Information Representative for the Postal Inspection Service in the New York division. And as soon as this comes back, I want to talk to you about what we call the stranger in your house, so the stranger in your home, which is all about deceptive offers.

Danielle Blakely:
Hold on one second, Donna. I'm sorry.

Donna Harris:
That's okay. So, it's two screens back, right.

Danielle Blakely:
Yep.

Donna Harris:
OK, it's all about deceptive offers. Every day we are literally opening the door and the window of our home to a world of strangers, who in fact, could be scammers. While in some cases, the resulting interaction is a positive one, but in other cases, the results can be devastating, especially to older and vulnerable adults. So, how does this happen? When you receive a pitch through the US Mail, text, email, and even by telephone, many of those offers, or interactions, are broadly referred to as deceptive. The look, the language, and the images used are deliberately designed to be misleading. And, even though many of these scammers are miles away, they can enter your home through deceptive offers, designed to steal your money or your financial DNA, and that would be things like your date of birth, your social security number, your mother's maiden name, those things that identify who you are. I like to call it financial DNA because it's just like your fingerprint or something that makes you, you. The stranger in your house can do an immeasurable amount of damage before the product comes to life. And, this is why we routinely discuss current trends and scams to make sure you are aware of what's lurking behind that next pitch, or that offer that seems too good to be true. This is even more important as you age. And, I'm in the older generation myself, but it's very important because the scammer doesn't care that you're older, that you're on a fixed income, that you may not have the funds to, you know, to continue

the way you live. All they care about is separating you for your money. That is their one goal. So, we have to be, I like to say: scams-savvy, because if we do that, then we are always ready for the next pitch that we can just hang up and not really fall victim to what they're selling us. Next slide please, Danielle. Now, as Danielle mentioned earlier, we've been cooped up for a while with the pandemic and everyone's looking to go on vacation, but we would hate for your dream vacation, you think you're getting what is in the top photo, but when you get there, you find out that it is really the bottom photo. So, I'm going to go over a few things that you should know about, a few scams and a few tips to make sure that you can avoid or to help you avoid this. So, the first thing is, with vacation rental companies like Vrbo®, Airbnb, they have become very popular. In the past, years ago, you rented from a hotel or you stayed with family and friends. But now that these vacation rental companies are out there, you have to be very careful of who you rent from. The first thing that you should do is always go online and do your research. Whatever search engine you use, look online to see if they have any complaints. As you are looking at the reviews, make sure that the reviews give you details. Wherever there is a review without many details, you have to ask yourself, is that really a paid review? So go online, look at the details, look at the reviews, look at what people said about the facility. If you're renting something you want to make sure that when you get there if you're renting an entire house, that there are not 15 other people living there, are you're not going to be staying in one little room with your family of five. So, those are some things to do. The other thing is to make sure you always use your credit card. When you use your credit cards, you have the protection of your credit card company. So, if your vacation rental doesn't turn out to be what you think it should be, you can always go back to the credit card company and dispute it. But, when you use your debit card, it's like using cash. And it makes it really hard, if not mostly impossible to get your money back and then you've lost your funds. Always know who you've rented from. Who am I actually renting from? Am I renting from a company or am I renting from an individual? If you're renting from a company or individually, it doesn't matter, but you need to know how to contact that individual in case there's a problem or things don't go as planned. And that's the one thing you need to make sure of when you're renting through one of these Airbnb, VRBO or one of these sites. Even when you're using a site such as Travelocity, Expedia, all those sites, make certain that you read the fine print. Another thing is free vacations. Now we've all been in a mall somewhere or received in the mail, a little card that says we're offering you a free vacation you just have to pay a $99 fee, a $49 fee, but there's no such thing as a free lunch. So, there's definitely no such thing as a free vacation. You may get there, but there is always another pitch. OK, I'm here on vacation, but I have to go to these four seminars in order to get my free vacation. Or, I need to pay another fee if I want to want to add another day to my vacation, or if I want to have food I need to pay this extra cost. It's always another cost or another fee. In some cases, that vacation package that is supposedly free that you're going to get in the mail never comes. So always be cautious with those, I like to say, with anything if I have to pay for something that's supposed to be free, then it isn't really free. Okay. Another tip is, there's travel insurance when you go and you have a vacation when you get travel insurance, make certain that your travel insurance is with a registered company, and not just some fly-by-night company. That's very important because if you have a problem you want to make certain that you can be reimbursed, and that the company exists and that you're just not paying your money to a scam. So, make certain when you look online and you get reviews. You can go to the Better Business Bureau, you can go to your local attorney general, the FTC and look online for, the signs and the tips of what a regulated travel insurance company will offer you. But once again, I always say, read the fine print. Now, I know you've all received robocalls relative to how it's a free vacation. Right now during this pandemic,

we are getting robocalls for everything. Hang up. It all sounds good, but if somebody's robocalling you, they call thousands of people. For a scammer, if they get two people to take a pitch and to send money, well they are doing well. If you think about this, if they make, I do not know, I'm going to use a small number because I know it's more than that. But, if they make 1000 calls, and they get 20 people to send them $100. Look how much money they got just from making those robocalls. And, they're not sitting there. Their machine is doing this for them and they are getting this money for doing very little work, but selling you the pitch. So, why I say, if I didn't call you and I didn't go out and look for a particular item when I get that call, I'm hanging up. Better yet, do not even answer it. There are services out there, we do not endorse any particular service, but the Do Not Call Registry as Danielle alluded to, but also no more robo, and now most mobile phone companies, they have spam filters on their calls to help reduce those calls so that one gets through, make sure you hang up. Do not give them the time to discuss with them, you know what their offer is because there is always a catch in that offer, and certainly don't give out any of your personal information. Another thing is rental car scams, so I'm going on vacation and I tried to rent a car and I've been trying to rent a car for quite some time. So, with the pandemic, a lot of rental car companies had to sell off some of their fleets to stay afloat. So, there are not that many rental cars out there and the ones that are out there are very pricey. So I looked in the range of rental cars for two weeks and they were in the range of $1,700 to $2,300, which is ridiculous for a rental car. But then I got an offer because as Facebook and other companies do and through algorithms, all of a sudden I get this offer in my email for auto rental deals. So I looked online and I said okay let me humor myself and look to see what this is going to actually be. So, for 10 days, I was going to be able to rent a car from Thrifty rental car for $230 that included fees and insurance because you know there are always fees with a car. But, if I had to really think about that, I always say trust your gut. Because my gut said, how can they give me this car for $230 for 10 days, but these other reputable companies cannot give me this car for less than $1,700. So while I wanted, on one hand, to go with this cheaper company. I said no because when I go on vacation and get off the plane, I want to make sure that I have the car that I wanted. So always use a reputable company when renting a car. Make sure it is possible to use your credit card. I know some rental car companies, let you use a debit card for a larger fee, but the credit card is key because you have the protection of your credit card company, and you can put that particular payment in dispute or that charge in dispute, and hopefully, you will not have to pay it at some other time. So the last thing I want to talk about on travel is a new scam, the hotel scam. It works similar to the grandparent scam, believe it or not. You check into the hotel and in the middle of the night, you get a call supposedly from the front desk, and the front desk person says well when we ran your card earlier today, we thought it processed, but it did not. So if you could just go over your credit card, give me your credit card number again so I can make sure that I have the correct numbers. Do not do that. Because they call in the middle of the night, just like the grandparent scam to confuse you, when you're not really thinking about what they're asking. And if you give your credit card number to that person, they're going to use your credit card to purchase all sorts of items that you did not actually purchase. So whenever you are confronted with an odd pitch or a solicitation or something of that nature. Just say, you know what, I'll come downstairs to the front desk, and I'll settle that right now, and that way you know if they call, or if they didn't because in most cases, they would always ask you to come down to the front desk. If that was a reputable front desk attendant. Could you go to the next slide, Danielle, please. Thank you. I talked about vacation scams and I'm just going to briefly go over the Phishing, Vishing, Smishing and Pharming. They're all basically centered around the same thing. It's an effort for a scam or a scammer to get your information using a reputable company. They could use

Apple Bank, they could use the Postal Inspection Service, the Postal Service, but you'll either get an email, a phone call or a text asking you to do something to either call, press a link or to do something so that that person can get your personal identifiable information. If you get a call from the bank. Hang up. The bank is not going to call and Danielle I'm sure you can verify this, the bank is not going to call and ask for your personally identifiable information. They already know it, okay. The Postal Service is not going to. Right now, I see that we are getting complaints about a text from the Postal Service, about a package. Well first of all, we don't know your cell phone number, so we can't really text you. All we know is your address. Those kinds of things are scams. Just hang up. If you have a question from your credit card company. Call your credit card company, look on the back of your card, call the number on the back. Call your bank, look at your statement, go to your bank. These are all ways to protect yourself from scams. Now I'm going to briefly talk about a lot of the issues. Elder fraud, unfortunately, is on the rocks, and I know many times I speak about these things, doing a presentation and someone will say well it's never happened to me I will never be scammed. Anyone can be a victim of a scam, no matter how old you are, how young you are, how much money you have, whatever it is you can be a victim because it's all based on the pitch. Lottery and sweepstakes, that's just another pitch. If you did not pay to play, it is not a state lottery, your local lottery, then it's a scam. Foreign lotteries are illegal in the United States. So, if you play in a foreign lottery, then you're part of that illegal activity. If you get a letter in the mail with a check attached to it saying hey you have won the lottery. There is $2,500 to help you for taxes and fees. Then deposit this check and send us the remainder. That is all the same. That check is counterfeit, but there is something about funds being available and funds being cleared. There's a difference between the two. The bank has to make your funds available, but that doesn't mean the check is cleared, so don't get stuck on the hook, paying for that check to deposit when it comes back not cleared. Romance scams like anything else. Everybody loves to be in love. But, you know, is it really true, if you actually meet someone and they start asking for money, or asking, you know, oh, I have a sick relative, I can't come see you. But I need some help. Can you help me? Can you deposit a check for me and send me the money? Don't fall for it, OK? If someone sends you a picture, put it in your search engine and do a reverse lookup, because I guarantee you that pictures been used hundreds of times. Okay, there's a good video it's called *Crime Without Blood* and it was made in the Netherlands and if you ever get an opportunity, review it. It's an animated quick video that just shows you how a romance scam can be so devastating to someone, both financially and emotionally. So, love is a great thing, but not when it leaves you with absolutely no money. Go to the next slide. And this is the lead list. This is what they look like. So when you go fill out your name to win free coffee for a week, or sign here to go on a free vacation, or for this investment seminar, your name gets put on a lead list. And these lead lists are very valuable because a name could be worth anywhere from $3 to $10 on the lead list. And this is how people actually call you and get your information. So, once again, no free lunch. Do not sign up for things that you don't really need and don't want. So that's it for my part, but we've got more about identity theft coming up with the next slide. Thank you, Danielle.

John Viola:
Good morning, everyone. My name is John Viola. I'm a postal inspector team leader. I supervise a team of federal agents and my team focuses on mail theft and identity theft investigations. I'm going to give a very quick overview of identity theft. I'm sure all of you have heard about identity theft. Some of you may have been victims of identity theft at one point in time. Simply what is identity theft? That's when someone gets a hold of your personal information, your credit card, your social security number, your debit card, your date of birth, your mother's maiden name. And what do they do with this information?

Well the first thing they do if they have your credit card or debit card, they can make purchases using these cards purporting themselves to be you. That could be online purchases, it could be in person purchases, a lot of these if they just have the numbers, they do online purchases using your information. What else can they do with your personal information? They actually could apply for credit cards in your name and credit in your name. Having these new credit cards, they can do online purchases very easily. Also, they can get the physical card, and then go to these establishments and purchase items in your name, purporting to be you. They can also file unemployment benefits or file taxes in your name, using your personal information. None of us like to receive bills, when you get them in the mailbox, it's not your favorite thing to receive in your mail but if you don't, if you stop receiving these bills, it may not be a good thing. It could mean that someone got a holding of your information and changed your address, either with the financial institution or with the Postal Service, and they're now getting your documents. And if they're getting it, they can apply for a credit card or have your account change over to their name. Now getting your information and getting your actual card. So what can you do to protect yourself from identity theft? The first thing you want to do is secure your financial data. Before you disclose your credit card or financial account numbers to anyone on a website, make sure that the website is secure or it has encrypted data transmission transaction. Check for the icon on the website window and you should see a lock. Now what you want to do is hover over it, and actually click on it, because what the fraudsters can do, they actually can take a picture of this and embed it into their websites. So what you want to do is click on and it should come up when you click on it saying that it's all secure. Another thing you want to look for is that it has the HTTPS, the "s" on that site means that it's secure. If it doesn't have an "s" that means you're on an unsecured site. So make sure that you're checking those before you enter any information. And also, don't go on a site that you're not familiar with. Make sure that it's a site you've dealt with you confirm that it's a legitimate site. Protecting your social security number. We only have one social security number, so want you want to do is protect that Social Security number as much as you possibly can. So what do you want to do? Only give it out when you must. As an alternative, see if you can just provide the last four numbers. A lot of organizations, a lot of companies now, businesses, will accept the last four, rather than you providing your entire social security number. And it's also reasonable to ask why this particular organization needs your social security number. I know a lot of times you'll go to a doctor's office or you'll go to a different location and they'll ask for your social security number on a form. Ask them if it is really necessary that you provide this, if it's mandatory or if they are going to still provide service without it. Also, whether you can ask them, what are they going to do to protect your information? That is a reasonable request and a reasonable question for you to ask. The next thing you want to do is obviously shred financial documents. Never throw any financial documents that contain any of your information into your garbage, you want to do is make sure you shred all your unwanted credit card applications, your canceled checks, your bank statements, any document that you have containing personal information, you want to make sure you shred. Do not throw it away as a whole. Next screen, please. So, what can you do to make sure or determine whether or not someone's obtained credit in your name and took over any of your accounts? You can go to annualcreditreport.com. And by going on there, there are three different credit bureaus that are out there, Experian, TransUnion and Equifax. You are entitled to a free credit report from all three organizations on a yearly basis. So if you apply for your credit report from each one, every four months, that means throughout the entire year, you'll be able to monitor your credit at no charge to yourself. So it's annualcreditreport.com Or you can also call the 800 number that they have the 877-322-8228. This information is also on the FTC, the Federal Trade Commission website. If you wanted to go to verify

anything, you can go there as well. Next screen. And the last thing you want to do to protect your identity ensures your mail delivery. Do not leave your mail in your mailbox overnight. I always tell consumers when we're talking to them is that if your mail is not in your mailbox, it can't be stolen. So, try to get it out of your mailbox as soon as possible after delivery. That reduces the opportunity of perpetrators taking it from your mailbox. If you're going on vacation, contact the Postal Service. You could do it either online or in person with a form and have your mail held. If that doesn't work for you, if you have a trusted neighbor that you can have or friend check on your mail and remove the mail from your mailbox daily. Like Donna mentioned earlier, it sends up the signal that you're not in town if it's in your mailbox. But it also enables them to get ahold of your information if it is in your mailbox. If you're mailing outgoing mail to pay your bills, the best way is if you can mail it at the post office. Inside the post office, in the lobby, there is what we call a lobby drop. Where it actually puts your mail into a slot, it actually goes into the Postal Service, into the back of where the employees work. If that doesn't work then you've got to mail from a collection box. I have the picture on the screen right now. It's one of the high-security collection boxes that we have out there. I think you've probably seen these out there. There is no longer the handle where you pull open that door and mail your letters. These actually have a slot, and these boxes are high-security collection boxes that are out there to protect your mail from theft. If you work at a location where you have a business or a letter carrier that comes to pick up your mail, you can also hand it to your letter carrier when they collect your mail there. That's another way to secure it. But I always tell people to, even with the high-security boxes, look on the collection box and see when the next collection time is. The best time to mail is in the morning, rather than at night, because if you are mailing at night you're putting your mail in the collection box at night, and now it's going to sit there until the next day when the carrier collects it. So look at the collection time, and if possible, if you are going to use any collection box, the best bet is to mail it in the morning, if possible. Next screen. So Donna if you want to interject a little bit too but the main points and mail fraud takeaways like I talked about identity theft, you know, protecting your identity, checking your credit, and ensuring that your mail is secure.

Donna Harris:
Right and just to follow up. Once again, as Danielle mentioned earlier: reporting. If we don't know about it, then we can't investigate and a lot of times people are embarrassed, they don't want to report it, but it's so important that we have that information because that's how we make cases. You know, it might have happened to one person over here and maybe that doesn't move to the level of being able to prosecute it federal. But as we see this continuing to happen we're able to put those pieces together, investigate, and bring these individuals to justice whether crimes, through prosecution through the state, in some cases, and other cases through federal, depending on the prompt. It's really important to report it. Never be embarrassed about being a victim. You're only a victim if you don't take charge and report these individuals because I guarantee you what they're doing this to you, they're doing this to someone. So that's, that's it for my tip. Danielle, I'll turn it back over to you now.

Danielle Blakely:
Yes, that is the end of the presentation, all the contact information is here for Apple bank, you can contact CustomerLine at 914-902-2775 and toll-free at 800-722-6888 and John and Donna's information is below as well. For any additional questions that you may have. And that is the end of our presentation and I will stop sharing my screen.

Lyman Clayborn:
Hey, it's Lyman. Thank you, Danielle, thank you everyone at postal, and everyone at Apple Bank. This was really very informative. There were some questions in the chat already. And one of those was about the recording that we're doing, of this. And I just want to say that the recording is given over to the library's editors, and they will edit it down and it will be posted on the library's YouTube channel but we will send the link to that to everyone who is on this call that registered. Was there a question that someone had, make sure to unmute yourself first, please.

Participant #1:
Yeah, I was trying to get Donna's information which is, she stopped sharing her screen and I didn't pick that up. Can it be put in the chat, Donna Harris?

Lyman Clayborn:
Oh okay, Danielle, did you want to share the final slide, number 29.

Danielle Blakely:
Yes, I will share my screen. Once again, my apologies.

Lyman Clayborn:
That's okay. There you go.

Participant #2:
Yeah, I just wanted to say one thing. Apple Bank's calendars are the best. And I wanted to tell you that and I have one hanging up and I always get your calendars. They got a little smaller but I really love your calendar.

Danielle Blakely:
Thank you. We appreciate that.

Lyman Clayborn:
I don't see any other questions in the chat. The Apple Bank customer service line is also in the chat. Does anyone want to unmute themselves like the other participants did with a question? We do have a comment, not a question in the chat who said, "Wow!!! This was an awesome presentation by all presenters. Thank you for all you do to service the community." Thank you.

Participant #1:
I do have another question. I was concerned back in the day that when we used to get packages delivered, especially to a private home if the package was too big to put into the mail, or through the gate, the postman will leave a tag on the door, and allow us to go to the postal office and pick the package up. It seemed that they're no longer doing that. Is there a reason for that? Is it the pandemic or they just stopped doing that service?

Donna Harris:
Do you want to answer or do you want me to answer that?

John Viola:
You can answer it Donna and I could interject if there is anything additional.

Donna Harris:
Okay, there are a couple of things associated that I'm going to give it to you from my experience because obviously I work for the law enforcement part of the Postal Service and not delivering operations. But, I do know that part of it is due to the pandemic, where they have changed some of their delivery procedures as a result of that. But also, you didn't mention, are they just leaving a notice, or they're just telling you that you have a package and to come to the post office. What are they doing, rather than just leaving your package?

Participant #1:
On some occasions they just leave the package and they don't ring the bell, or nothing so I don't know that the package, being in a private home, having two floors, I don't know that the package is delivered. So, I might go out and look downstairs and see there's a package sitting out in my gate which is cause for thievery. You know shopping in the neighborhood, as I call it. Two things, they should ring the bell, and somebody is home go outside and pick it up. Or if you're not home, don't leave it, they will take it. Leave us a note, a tag they call it. We will come to the post office and pick it up. I have notes all over my house upstairs and downstairs, "Please do not leave a package, I will come to the post office." Which is close to me, and pick up the package. They ignore that, you know, a sign on my door and leave it. And then sometimes I get it, sometimes I don't. And try to find a company to replace a package. You know, it's sometimes very hard.

Donna Harris:
So what my suggestion is, that if you email me your name and your address via email, I can send it to the station that will cover your area. Now, I can't promise that they're going to make that change because of this pandemic and the way that they changed some of their delivery operations, but I can bring into the manager's attention that you would prefer that your packages are not left. Just join your staff if you're not there to hold them at the post office so I can call and have someone contact you and email your information.

Participant #1:
Well thank you, but I know of your name from prior. So that's why I'm talking to you.

Donna Harris:
Oh, okay, yes.

Participant #1:
I know your name Donna Harris from previous. Thank you.

Donna Harris:
I will do the best I can to, you know, give them this information.

Participant #1:
Okay.

Donna Harris:
Hopefully, they will, you know, hold the packages at the post office. Okay.

Participant #1:
Thank you very much.

John Viola:
And we will also notify the mail dev team that covers your area to let them know that you've had a problem there with the parcels in the past so they're aware of it as well.

Participant #1:
Thank you, John.

Participant #3:
I had a problem myself so.

Lyman Clayborn:
Yes.

Participant #3:
And thank you John for talking about it because what this special postal man, he comes and rings the doorbell and by the time I get there, I see him walking away. Then I look down and there's a package. He does not wait to deliver it to me. He does not wait for the person to answer the doorbell.

Donna Harris:
Right.

John Viola:
Yes, the same thing that was just said previous. If you are having a problem where you are not always home or if there's a problem with theft in the area we could definitely let the station know that we're requesting that you just want to see if you were home at first. The carriers there, they are under a lot of time constraints so they're out there trying to get their routes done as quick as possible. It's not an excuse for them but if there is a problem where, by chance, you do not want the parcel left there at all, we can contact the station for you and put in that request and let them know that you've had some issues as well.

Participant #3:
But it seems like it is a general problem because I thought I was the only one having the problem.

Participant #1:
I like Sunday deliveries though. The Sunday deliveries with the truck is good. They deliver on Sundays because most homeowners are home on Sundays. Thank you.

Donna Harris:
Well, yes. And, you know, from the standpoint of the Postal Inspection Service, we play a role, as you could say a liaison, a consultant to the postal service. While we are part of the Postal Service, we are one of their law enforcement. They have a law enforcement entity, which is the Postal Inspection Service, and then they have a more of an auditing body, who handles more internal crimes, and that would be the Office of Inspector General. So in this case, what we can do is, John mentioned, I think we can send your information to the Postal Service, and ask them to either reach out to you to follow your request, we can certainly can do that. Well there have been some changes to the delivery of funds for employees. But as John mentioned, they're under a lot of stress, to get packages more and more and more packages delivered. But no excuse, they should deliver as you require and we will pass this

information along to the stations that cover your areas. if you if you email me, I can pass that information along.

Participant #3:
Thank you.

Participant #4:
Hello.

Participant #1:
Thank you.

Participant #4:
Can I talk? Hello.

Donna Harris:
Yes.

Participant #4:
I live in an apartment building. I have the same problem. They don't even ring your bell, they just put the package right in mailboxes. And they steal it, they steal packages in my building. They don't ring your bell. How come they don’t bring it upstairs and put it in front of your door?

Donna Harris:
I do not know why they are not doing that.

Participant #4:
None of them are doing that. UPS, United States Postal Service, name it. Nobody brings your packages up. They do not even ring your bell. They just put it down there, that is it, and I have packages stolen all of the time.

Donna Harris:
Do you have an email? Can you email me?

Participant #4:
Yes.

Donna Harris:
Email me your information and I will report it to the station that covers your area. And certainly, I'll forward it to the inspector of the team leader that covers that area relative to mail theft and things that relate to the Postal Service. Why their deliveries have changed, I can only say it's the pandemic.

Participant #4:
No, they did that before the pandemic.

Donna Harris:
I can't answer for them because I work for their law enforcement, but certainly I'll pass your information along.

Participant #4:
Okay, please. Thank you, I appreciate it.

Donna Harris:
Welcome.

Lyman Clayborn:
Thank you. Thank you. Before we go, because we have maybe one or two minutes. There was a question from somebody in the chat, what should be your first course of action if you feel you have been a victim of identity theft? This will be our last question today.

John Harris:
Yeah, well the first thing you want, if you've been a victim of identity theft, if you know the accounts that have been affected immediately, is contact those credit holders, let them know that you are a victim, have those accounts shut down. Also, you can put a credit freeze on your account. If you're a victim of identity theft, it's no charge if you're a victim. File a police report, file if someone took over your account for the mail. If they had your mail redirected, file with the Postal Inspection Service. You could do that online as well. Notify us of it but the credit freeze, what that will do, is prevent anyone from getting any new credit in your name. It is a very good tool out there and you will have to file it with each individual credit agency, Equifax, TransUnion, and Experian, but if you do that no one will be able to apply for credit in your name. So, if you secure all of the accounts that have been affected, prevent anyone else from getting back and a new, new numbers assigned to you, they'll prevent anyone else from getting additional credit in your name.

Participant #5:
Thank you. I appreciate it.

Lyman Clayborn:
Thank you, John. And let's give a virtual round of applause to Donna Harris, John Viola and of course, Danielle Blakely with Apple Bank. Thank you so much to Apple Bank today. Thank you to the US Postal Service. This was really a great and informative program. And thanks to all of you patrons who showed up today. We really appreciate it and we look forward to having more exciting and interesting informative library programs for our older adults. So thank you and have a good day.

Patrons:
Thank you.