Pandemic & IRS Elder Financial Abuse
Fact….or Fiction?

April 2021

Lyman Clayborn:
Good afternoon, everyone. Hello, I'm Lyman Clayborn. I am the Coordinator of Services for Older Adults for the Brooklyn Public Library. Thank you so much for coming and joining us this afternoon on a very, very special session and program from the library: Elder Financial Abuse: Protecting Yourself from both COVID and Income Tax Scams. I would like to thank my colleagues on this call, Judy Vigo and Samantha Dodds, for helping me today to coordinate this program. I would like to remind people to please remain on mute. There is a question and answer section at the end where you can unmute yourself and ask questions. Otherwise, you can put questions into the chat, and I will monitor them, along with Judy and Samantha, so that we can give those questions to our speakers at the end. I do, however, need to tell you this program is being recorded, and anyone who does not wish for their image or voice to be shared as part of our broadcast, please turn off your camera and microphone at this time. Additionally, please be aware your name may appear in your Zoom window. So, we did want to give you a heads up this is being recorded and may be shared on Brooklyn Public Library's social platforms. So, without further ado, let's get into our program. 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 continuously strives to improve the quality of life in our neighborhoods through community involvement as well as personalized financial services. Apple Bank sponsors a wonderful array of Brooklyn Public Library programs and services annually, including multilingual family programs and beloved programs for older adults, like our Creative Aging series. Today, Apple Bank and their partners at the Internal Revenue Service are joining us to talk about our partnership on a special event to help educate and protect members of our community from financial scams. It is my pleasure to first introduce Jefferson Nicholls from Apple Bank, Senior Investigator for Fraud Prevention and Investigations, to tell you more about this event. Thank you.

Jefferson Nicholls:
Thank you to everyone for attending today's presentation on pandemic and IRS Tax Elder Financial Abuse. Once again, my name is Jefferson Nicholls, Senior Investigator for Apple Bank. I would like to thank the Brooklyn Public Library for sharing a platform to allow our presentation. Before we begin, I would like to introduce the chairman, President and CEO of Apple Bank, Mr. Steven C. Bush.

Steven C. Bush:
Thank you, Jefferson. And I, too, want to thank Chris Westphal and the IRS team and the Brooklyn Public Library for organizing this event. And it's an important topic on elder abuse as it manifests itself through the financial system. As Lyman said, Apple's been around since 1863. I haven't been here all that time, but I've been at the bank for about 30 years and have really been pleased to see - since the late 90s - our expansion in Brooklyn, where we've got quite a few branches. Throughout that time, we've been pleased to serve the New York community generally, Brooklyn specifically, and very happy to be partnering with the Brooklyn Public Library on a variety of public affairs topics. Unfortunately, our topic today of elder abuse is something that we see on a daily basis at Apple Bank as the pandemic has created new and different kinds of scams that are targeting elders. It's also forced more activity into a remote setting through electronic banking, even forcing more ATM transactions.

We've tried to stay open as much as possible for normal person-to-person banking, but certainly we've had - and we continue to have - cases where branches are shut down for a period of time because there are COVID cases among our staff. So, as banking has had to move away from its traditional in-person format, we're seeing many new kinds of attempts to target elders. So, it's important at the bank for us to do everything we can to stay educated on vulnerabilities and on scams that we see with our customers, to keep your antennas up and to try to protect you. But oftentimes, because of the remote nature of some of this, it's hard for us to know. And occasionally, we find ourselves challenging the children of elders on their rights to have a conversation about an account, because we're worried about elder abuse, and these can be challenging conversations. So, we're doing our best, I think the other banks, who are colleagues, and financial services are doing their best. But one of the best places to start is for you to have the best knowledge on what types of fraud awareness you need to have so that you can help alert us and help us use that knowledge to help protect others. So, with the help of Jefferson and the team within our compliance area, and Chris has experienced this field with the IRS, we hope that you get some real value out of today's presentation. And it helps to open your eyes to both new and the many old scams that continue to work to prevent you from falling victim to that sort of event. So, thank you all for attending. And we hope that you'll enjoy this webinar and confined environment.

Jefferson Nicholls:
Thank you, Mr. Bush. Welcome everyone, once again, for those who are joining us right now, I am Jefferson Nicholls, Senior Investigator for Apple Bank. A little bit about myself: I joined Apple Bank in October 2020. Prior to joining Apple Bank, I held various roles and accomplishments, some of which involve fraud prevention, conducted internal and external investigations, physical security, certified active shooter trainer, security manager, oversaw and provided direction for major security-related projects during the implementation of various security technology systems. Joining me today is Supervisory Special Agent for the IRS criminal investigations, Mr. Christopher Westphal. Please tell the audience a little bit about yourself.

Christopher Westphal:
Thank you, Mr. Nicholls. Good afternoon, everyone. Thank you everyone for inviting me to today's presentation. Again, my name is Chris Westphal. I'm a Supervisory Special Agent for the IRS Criminal Investigation. I've been with the IRS Criminal Investigation for about 13 years now. I started my career out of the Washington D.C. field office, where I worked on a number of varieties of different criminal investigations relating to tax and tax-related financial crimes. I recently moved up here to the New York field office instead of our hub office, which is on Eastern Long Island. And I've been here for about a year. And looking forward to speaking to everyone about the scheme's trends and some tips and tricks that I can share with you all and combating the COVID related and stimulus check frauds that we're seeing.

Jefferson Nicholls:
Thank you, Christopher. The COVID-19 pandemic, which we are all experiencing, has caused us to make many changes to our normal life routines. However, as we continue to learn more about the virus and the vaccines available, we hope that our presentation on pandemic and IRS Types Elder Financial Abuse will raise more awareness of various scam activities targeting older individuals.

What is elder financial abuse? Elder financial abuse is the illegal or improper use of elders' funds, property or resources by another individual. These individuals prey on the elderly for their own financial gains. These ads are unauthorized and immoral. The impact of Elder Financial Abuse, the financial exploitation of the elderly, contributes to more than $3 billion in losses annually, which can cause serious health risks, such as physical complications and mental health issues. This is why a majority of the elder financial abuse cases goes unreported and fraudsters evade prosecution, allowing them to continue to exploit the elderly. However, if the victim so chooses, and criminal charges are filed, financial elder abuse can lead to misdemeanor and felony charges. Misdemeanor convictions can lead up to a year in jail and $1,000 in fines. Felony convictions can result in up to four years in prison and fines up to $10,000.

One of the prominent elder cons involved is the COVID-19 stimulus checks and unemployment scams. They are very lucrative, and fraudsters love them. For stimulus checks, they recruit the victims with the belief that they can really receive their payments early by providing your personal information. Once they receive access to your personal information, they apply for unemployment benefits with pictures and the victims' names, which leads to identify theft.

For those who have received your vaccination, you're already familiar with the vaccination card. For those who have not been vaccinated, this is what the card looks like. Possibly, most of you have seen it posted on social media. Posting this card on social media can also lead to identify theft -- do not share your personal information, medical or financial information with anyone claiming to offer money or gifts in exchange for participation in the COVID-19 vaccine survey. Be mindful of how you dispose of your COVID-19 vaccination costs. Improper disposal of this item can be used by bad actors to commit fraud. In addition, beware of mobile sites offering free COVID-19 tests. Only use an approved testing site, which can be found on the NYC.gov website.

These mobile sites can be operated by fraudsters to collect your personal information and provide inaccurate testing results, such as informing you that you tested negative when actually you could be positive and vice versa. They may visit assisted living facilities and offer medical services in exchange for Medicaid and Medicare ID numbers to commit fraud. Remember, legitimate contact tracers will never ask for your Medicaid number, financial information or attempt to set up a COVID-19 test for you and collect payment information for the test. So, fraudsters are in plain sight, but usually appear invisible, because fraudsters can be trusted individuals, such as landscapers who overcharged the elder for services because the elderly cannot complete the work themselves. Also, fraudsters can be next door neighbors who appear to be assisting with daily tasks. For example, running errands, food shopping, picking up prescription -- but lie about the cost. In addition, some trusted companies that provide assistance for the elderly may have a rogue employee who befriends the elder and commit elder financial abuse. For example, the rogue employee says it'll be easier for them to conduct the transaction and request the pin number for the elder's debit card, which leads to unauthorized transactions on the elder's account.

At this time, I'll turn over the program to our guest speaker, Christopher Westphal.

Christopher Westphal:
Thanks again, Jefferson. And to circle back, really the purpose of today, in addition to add on to Mr. Nicholls, is to provide from the IRS Criminal Investigations perspective, what we're seeing locally as well as nationally in terms of the schemes and trends relating to the cares act, stimulus fraud, tax fraud and general crime as a whole. The IRS Criminal Investigation, everyone's heard of the IRS, is one of the largest government agencies. We, the IRS as a whole, employ about 80,000 employees. Of the 80,000, 3,000 comprise of IRS Criminal Investigation, the sworn law enforcement arm of the IRS. We're sworn law enforcement officers, we're authorized to carry firearms, execute in effect, search and arrests and interview.

So, our objective is to identify our evaluate allegations of tax and related financial crime in terms of determining whether or not those crimes are valid and warrant prosecution. We work hand in hand with county state and federal law enforcement partners and agencies, with our local U.S. attorney's offices as well. And we're really focused on the egregious tax evaders and fraudsters out there. We're not focused, or our primary goal is not on administrative or technicality type issues, we're looking for egregious facilitators of crime, and or people that are committing the crime, whether failing to report income in an egregious, willful and purposeful way. So, that's really what distinguishes us from the IRS as a whole, where we have a very specific purpose and mission. We're the only law enforcement agency already to investigate and recommend prosecution for tax crimes. And in addition to being the supervisor out of the hub office, we have offices throughout Long Island throughout Downtown New York City and all five boroughs. So, we do have a pretty large presence throughout the New York Metropolitan area, as well as throughout all of New York State. Aside from being the supervisor, I'm also the COVID coordinator for the New York field office.

So, what I'm responsible for doing is I'm the intake for all potential COVID related scams. You may have heard of paycheck protection, the Economic Injury Disaster Loans and, of course, the stimulus check fraud that we are seeing. So, I intake that, evaluated and assign that throughout the field. We also work with the U.S. attorney's offices who have task forces specifically designated for working on COVID-19-related scams and those types of schemes. We're also working with other law enforcement agencies, because, generally, what we're seeing, the types of scams that we're seeing, have existed for quite some time, it's just COVID fraud, stimulus checks, Care Act. That's the area of susceptibility of vulnerability, the moment fraudsters have tailored their romance schemes or work from home schemes to address this pandemic and efforts to obtain ill-gotten gains. So, on the present slide, there are certain types of COVID scams: we have healthcare scams, stimulus checks, fake websites, robocalls.

One thing to know from the IRS, as well as any government agency: if you ever receive a phone call in which you're threatened of imprisonment, or that you need to make an immediate payment, that is outright fraudulent. I myself have received calls from the IRS stating that I owed an X amount of dollars and that if I did not pay by the end of the day, some officers would be at my door to arrest me. That's just not the reality.

And we've also seen with other agencies, the FBI, Department of Homeland Security, representatives acting on behalf of those agencies, which is just not the case. These schemes are outside of telephonic or robocalls. They also try to contact potential victims via email, via text, using a lot of electronic media that we have available to us today. The IRS will never reach out to you via text message or email. The IRS historically and traditionally, by way of our process, reach out via mail, and you will receive mailings – multiple mailings and notices – leading up to a potential phone call. So, just know that of all of the ways in which the IRS will initially reach out to you, none of which will be over the phone, there'll be no demand for payment, or anything of that nature.

Some of the stimulus check frauds that we've seen is, as of right now, we're on the second round of stimulus checks. And by and large fraud is perpetuated on the onset, meaning before the paychecks or the stimulus checks are received and afterwards, predominantly fraudsters are trying to reach out to victims via email, via text, advising that they can help facilitate the servicing or processing of your stimulus check for a minimal fee. That's outright fraudulent. And no representative of the IRS is going to be doing that. By and large, your stimulus check is based on your personal income tax filings from 2018 to 2019. And what you filed will be the determination of the amount that you receive in terms of your stimulus payment. And if you did file, those payments will be sent to the bank account that you submitted on either of those tax returns. Now, if you didn't file for 2018 or 2019, the e-taxpayer will receive a physical check which will be mailed to the last address on file with the IRS.

Now, this is where, aside from the beginning, when individuals contact taxpayers or victims essentially trying to either (1) get a fee for allegedly processing their tax return or their stimulus checks, or (2) trying to obtain bank account information PII (Personal Identifying Information), such as your date of birth, Social Security number, things of that nature, where they can use that and then take that and apply for a credit card or apply for a loan or something where they're going to use your personal identifying information for no good.

So, that's on the beginning, on the frontend of it. Now, fraudsters are in the know of treasury checks that are being mailed out. We've seen instances where fraudsters have contacts within the U.S. Postal Service mail carriers to where the mail carriers will provide the fraudsters a heads up as to which block or which neighborhood appears to be receiving treasury checks on certain days. So, the fraudsters will use that information and essentially surf up and down the streets, looking for those treasury checks. They'll then literally steal those treasury checks, wash the name off of that, and then negotiate at a local bank, something like that or to that effect. Healthcare fraud scams: we've seen that on some websites offering fraudulent cures for COVID-19, a guarantee to kill the COVID virus. That's outright fraudulent.

We've also seen where there's actual goods being sold, but they're knock offs or they're just general hand sanitizer where they're falsely representing that this is a cure. And in fact, it's nothing to that effect. And then the client or the customer, the victim is thinking that they're buying a genuine cure for COVID, when actuality it’s not.

Another instance is when they pay for a product, and that product never arrives. You see that's outright fraud. Other schemes that we've seen throughout the country and locally are charity scams. What we've seen recently is charity scams where an individual represents that they represent a charity, and they offer a job opportunity for an individual. We see this at work from schemes, or schemes in which individuals are looking for a job through an online job posting. They see the opportunity to work there, so they began working for the charity. And, in this particular instance, the individual would be receiving funds and the organizer of the charity asked that the volunteer provide their bank account information for purposes, facilitating receipt of charitable donations, and then that new volunteer would be asked to submit those donations to another individual. And in return, the volunteer would receive a small stipend, say $100.

And unbeknownst to that volunteer, the volunteer is considered a money mule and they have unknowingly participated and engaged in a fraudulent scheme or fraudulent enterprise. In actuality, there was no charity at all. But the individual was involved in narcotics and was using the proceeds and funneling those proceeds through this volunteer, unknowingly using their personal bank account, thereby washing the money and then that money being made from the volunteer to another business entity and the volunteer was none the wiser, but that was actually what was happening. So, I say all that for purposes of in today's day and age, where electronics and social media use of the Internet has been pervasive, many more people are working online, and job opportunities are being presented online.

When a potential job opportunity is presented and they're beginning to ask you for specific information, such as bank account information, your date of birth, Social Security number, with very little substance, be very leery and always be cautious of submitting your personal information via online.

Another instance to be cautious of is that many times these work-from-home schemes or fraudulent schemes are facilitated online or using general websites such as Hotmail, Gmail or those type of web-based email service providers. For me, that would raise a red flag, and you'd want to be a little bit more cautious moving forward. Any representative from the IRS, or any representations from the IRS, would never come via IRS.com. It's always IRS.gov.

But again, any representations or contacts from the IRS are going to be via traditional mail correspondence. Here, we see scams targeting taxpayers. Here's the phishing, the IRS impersonation email. Similar to the robocalls, individuals are demanding immediate payments stating that there's going to be threat of levies and garnishments of arrests immediately. That's just not how the IRS operates. Those same tactics, over the phone or via email. So again, be cautious of that and also be cognizant of the emails that appear very legitimate. And what we've seen is the emails themselves have actually progressed to appearing very legitimate. There may be an IRS[space].com or IRS as a very slight deviation. On the very first glance, it appears legitimate. I mean, even the language within the emails seems very official, whereas prior to that email, the language within the email itself appear to be written by someone who speaks English as their second language. And it was relatively easier to spot but, the scams themselves have evolved and the language and the way in which they're presented has evolved and appear much more legitimate.

Outside of IRS criminal investigation, again, because we're different, we're law enforcement officers, we do from time to time, and frankly, often, we will reach out to a witness or someone. We will approach someone at home or at their place of work. But we will always make it clear who we are, what our purpose is and provide our credentials. The same from someone on the civil side, whether it be a revenue agent or revenue officer, they should provide their credentials. And it's called the HSPD card, which is a laminated federally-issued government ID card, they should have that on them. You are within your rights to ask for production and their badge number, but we have a 1-800 number to call if you have any reason to question authenticity or the legitimacy of that individual. You can contact that number based on the information that the individual has provided to you, or verify whether they are who they say they are. Right. And this goes again, in terms of impersonations and the IRS making representations: The IRS will never demand payment from you on the spot. There's no surprises, this is oftentimes the audit process. The collection process on the civil side takes a significant amount of time and [after] numerous notifications have been sent, meetings have been held in person [or] over the phone and it's progressed either to a resolution or a dispute. And, at no time does the IRS ever request or demand that payments be made in cash or in debit cards or prepaid debit cards. No threats of arrest, nothing to that effect. Anytime someone is making those representations, it's going to be fraudulent and illegitimate. Payments will always be issued to the Department of Treasury.

If anyone is asking for payments to be made anywhere else, red flag should be going off immediately. And all these scams out there right now, COVID fraud, stimulus checks, Cares Act fraud, any sort of remedies, health care fraud scams related to COVID, they're all designed to either get money from you immediately, or to obtain your PII: your personally identifying information. It is just as valuable, if not more valuable, than the actual payment the fraudster can steal from you because from obtaining your Social Security number, your date of birth, your address, that information. They can then go and apply for bank loans or credit cards and really do significant harm to you and your financial status. In terms of what will harm you and your ability to move forward and if you want to obtain a loan, obviously, that prevents you from having the ability to do what you would like to do financially. It's prudent that you annually check and continually review your own financial statement, identify any suspicious transactions or any credit cards that may have been applied that you have no knowledge of, and it's really incumbent upon the individual to remain on top of that.

There are some websites that you can utilize such as ftc.gov. For your annual credit report each year, each of us are permitted to receive three free credit reports from Experian TransUnion and those bureau agencies and with that you can identify what credit cards or accounts you have open, and anything suspicious, you can then move forward and try to address.

Jefferson Nicholls:
Here are some red flags that we should be aware of when it comes to elder financial abuse. In the financial industry, we always train our employees to look for unknown persons or relatives or anyone suspicious coming in with the elderly to the bank to do banking transactions that we have never seen the elder with before. Sometimes these individuals we identify, we might take the elder aside to ask them questions, such as who is accompanying you today to the bank. Sometimes they say it's a caretaker or relative or friend. Those are huge red flags that prompt us to ask more questions of the elder to [determine whether] the person that is accompanying them that we've never seen before is either legitimate or a fraudster. So, we have to differentiate who that individual is accompanying an elder once they do come into one of our branches.

How can we help? That's a great question. When it comes to protecting the elder in the financial industry, we always try to find either a family member, or someone that can accompany the elder, maybe if there's a joint party, or even if there's a power of attorney to help assist the elder. But if we see any unusual activity, such as the elder is writing checks that are out of the norm, or they withdraw money that is above the normal limit. Like if the elder always takes out a couple hundred dollars a week, and now that's escalated to $2,000 a week. Those are usually red flags that alert us at the financial institutions to immediately speak with the elder. See what is going on and make sure everything is okay and try to take a deeper dive to make sure everything's on the up and up.

On this slide is great information where we can, as individuals, reach out, continue to educate ourselves, [through ways] such as this presentation to gain more knowledge and educate ourselves on how to recognize elder financial abuse. Scams targeting Social Security benefits, credit freezes, credit scores, identity theft webinars and fraud protection for older adults, which is very important.

Here is one of the most recent regulatory presentations on how to prevent elder financial abuse. If you have time, there's the link that you can have, the fdic.gov. That's where you can go on also and receive more information regarding elder financial abuse and regulatory assistance.
Also, this is another great website, www.dfs.ny.gov, and they have a lot of information for elders, such as the APS department (Adult Protective Services), which is a dedicated government service to help protect the elders, where they reach out to the elder. Before the COVID pandemic, they would visit the elder's home to conduct interviews, to make sure that all of their financials are in order, and no one is trying to take advantage of them.

Here is some other agencies that I've mentioned throughout our presentation. We have the New York State Department of Financial Services. We have the New York State, once again APS, the Federal Trade Commission, that's a great website to also go on and report identity theft.
If you're a victim of identity theft, you could go on their website, and you can file a complaint, and they'll reach out to you to receive further information on what your complaint is in regards to.

Here's some more great information on the FDIC website. Once again, they have an abundance of information that you can soak up, so you can educate yourself also to help protect your loved ones.

Here's our contact information for Apple Bank. We have our customer service line, and we have a toll free number. Also, listed is the contact information for Supervisory Special Agent, IRS Criminal Investigations, Mr. Christopher Westphal. This presentation is very important to us here at the Bank. We're very cognizant of all the scams that are taking place in today's environment. Everyone is looking to [unclear audio]; they're looking to make a quick buck. They're looking for the victims every day. They're digging deep, pulling all the stunts and all the tricks in order to take advantage of someone who's unaware of what they are billed, or even tricking the individual into thinking something's legitimate, so they can benefit from them. So, I hope this presentation was very beneficial. And once again, our contact information, if you have any further questions that you might have later on, we'd be glad to answer any questions or provide any further guidance if needed.

Lyman Clayborn:
Jefferson, hey, this is Lyman. There was a question for you and Christopher in the chat that I can read to you, if that's okay? Question: Paying legitimate companies by telling the customer service employee a debit card number over the phone. How to guard against rogue employees who may be working, taking orders over the phone, keeping their debit card number and later using it fraudulently?

Jefferson Nicholls:
That's a great question. Rogue employees are hard to identify until they finally use your card, and you report it. Usually there are regulations, regulation D that protects the consumer. So, you are protected under certain federal guidelines to help protect you from rogue employees that are using information. That's why it's great to also check your statement if you have online banking. As soon as you make a purchase, I would suggest that you check your statement online regularly. Check once you receive your bank statement in the mail, if you're still receiving it by mail. Also, review that immediately to see if there's any unauthorized transactions to help protect yourself. And once again, if that happens, go to the FTC (the Federal Trade Commission), website and file a complaint and provide all the details so they can also investigate that company that had the rogue employee, and hopefully that will also lead to prosecution for that rogue employee.

Christopher Westphal:
To add on to Mr. Nicholls, I completely agree it's best to be prudent and proactive in terms of providing your information. During that, you continue to look at your charges, there are certain tools or resources that certain banks provide, such as allowing notification of expenditures in excess of certain amounts. I know that's an option. In regards to providing your debit card information, one thing I've seen is that often the victim is contacted first and asked to provide their debit card. I would be suspicious on the outset if an individual reaches out to you, or a company. And if you're presenting to be from a legitimate company, soliciting your debit card information, of course, I'm sure that should raise a red flag. But on the other side, if you're reaching out to legitimate businesses, and requesting to make a payment, often there's certain checks and balances leading up to actual payments, you're writing your name, identifying you based on your account number, and you know that it's a legitimate business. Again, if it's a rogue employee, like Jefferson said, it's tough. We have to, in one sense, rely on the internal controls and business, but also the victim should be prudent and be aware of any suspicious charges and continue to check their bank statements. We had an instance where a dentist office's client records were compromised. Based on all the client applications and health information that was disclosed, they took that information, were filing false tax returns, false credit card applications. It just takes one individual to compromise an entire system. One would think that, you know, dentist's office wouldn't be compromised in a way like that. Criminals are as creative as anyone else. And sometimes, you know, it takes us some time to catch up to that. But the best advice is to remain vigilant and stay on top of your own finances and try and safeguard yourself as best as possible.

Jefferson Nicholls:
Here at Apple Bank, you can sign up for text alerts which will give you notifications of transactions processed on your debit card, where you can verify those transactions. Also, we have a monitoring center that will contact you via phone to verify if you did conduct transactions. So, we do have controls here at Apple Bank to help prevent rogue employees from having a field day with your debit card.

Lyman Clayborn:
The second question I saw in the chat, Jefferson and Christopher, says, if I have a parent living in Florida who is starting to experience some cognitive decline, are there basic instructions to give to her regarding avoiding abuse?

Jefferson Nicholls:
Yes, there is. I, just personally since my mother recently retired two years ago, we did have a parent-son conversation where I did explained to her about things such as spoofed calls. Also don't respond if you receive suspicious mail, just put it in the shredder. If you're online when you're banking, do not click on any suspicious pop-up screens. So, there's ways to also help protect the elderly by just making them aware of what's out there, what's going to happen, as we've also experienced ourselves when being online. If we're going to the bank, always protect your PIN number. When you're at an ATM, don't share information.
Protect your checkbook number, just all about protecting your personal information. Provide this information to the elderly.

Christopher Westphal:
To add, it's kind of a bit of a digression, but another scam or scheme we've seen recently in regards to Mr. Nicholls discussing and protecting your information is, unemployment claims or theft of your PII and filing fraudulent unemployment claims in other states.
The impact there is that we're seeing victims receive notifications in the mail of income earned from other states. Now the problem there is twofold. One, you've been a victim of identity theft. Second, is that now for tax filing purposes, the victim is on the hook or appears to have earned income in another state. Generally, the way to resolve that or at least begin addressing that, if you do receive a notice that you did receive unemployment benefits from another state, is to contact your local police department, file an official police report. They will contact the IRS as well as contacting myself. There are specific forms. There's an identity theft affidavit. So, you're going to want to do those two things, as well as work to schedule an appointment with your nearest IRS Taxpayer Assistance Center, because right now, due to COVID, it's on an appointment basis. But if you visit irs.gov, there are multiple locations throughout New York City and Long Island. So we're in the midst of filing season and were extended until mid-May, but we are seeing an increase of individuals that are receiving notices that they received income from other states when they had no business that are just outright fraudulent. So those are some of the remedies on the onset that you can do to protect yourself and address that sooner rather than later.

Jefferson Nicholls:
Yes, just want to touch a little bit on where Chris just finished. My department, Fraud Prevention and Investigation department at Apple Bank. On a daily basis, we are reviewing reports to see if anyone is receiving unemployment benefits in someone else's name instead of theirs. So just to let you know, Chris, here at Apple Bank, we are doing our due diligence as far as unemployment fraud.

Lyman Clayborn:
Thank you both. So, does anyone want to unmute themselves and ask a question? Just also keep in mind that we are recording this, and we are recording on speaker mode. So, if you don't want yourself or your name shown, you can turn off the camera but if anyone has any other questions, please feel free at this time to unmute yourself and ask Christopher or Jefferson. We have about nine minutes. Thank you.

Participant 1:
I have a question. How do they get our phone numbers? If we're not listed in the white pages or in the phonebook or things like that? How do people get the numbers to do those robocalls?

Jefferson Nicholls:
One way they can receive it is through a third-party relationship. Let's say before COVID, you go to the mall and sign up to win that car. See, you signed up, you put your information in there. Sometimes with the third-party relationship, that is how your phone number can be sold to the other vendors.

Participant 1:
Thank you. I was very curious with how they get people's numbers. Okay, that's, interesting.

Lyman Clayborn:
Thank you, Harold. Anybody else have a question for Jefferson or Christopher?

Jefferson Nicholls:
I just want to touch again on a personal note. If you are going to assist elderly, whether it be a family member, I suggest doing your own background screening on the individual, just to make sure that you know that everything checks out. Because remember that person is going to be with your loved one on a daily basis. So, you want to make sure that person's identity is correct and their background adds up.

Participant 2:
I have a quick question. You mentioned the unemployment scam. Is there a place that we call about that?

Christopher Westphal:
If you do find yourself a victim of this type of scam in which you receive notice from whatever state that you received unemployment, that the first step is to contact your local police department and file an official police report. There will be an identity theft affidavit that they should provide to you, which you will submit to the local police department. Then, there's a number of different ways to move forward. One, get Department of Labor to reconcile things on their end because obviously, this is incorrect and there is fraud here. The other part is that the IRS issue needs to be resolved because the state will file a record with the IRS showing income having been earned.

Then when the victim goes to file their tax return, not reporting that unemployment income will trigger a correspondence audit. Meaning you'll start receiving notices. If someone's a victim of this, it's prudent upon the victim to contact local law enforcement and to reach out to the IRS Taxpayer Assistance Center. And, like I mentioned earlier, there are a number of different physical locations, where you can set up appointments, and start that process of putting the IRS on notice. They'll provide further instructions as to how to go about resolving that.

Participant 2:
Great, thank you so much for that information.

Lyman Clayborn:
Thank you, Patti, for your question. And thank you, Jefferson and Christopher. There was a question about will the slideshow be made available? Yes. I will email that to everyone who registered for the program. We are looking at about four minutes till. Is there anyone that has maybe one last question for Jefferson and Christopher? Thank you.

Participant 3:
Thank you very much.

Lyman Clayborn:
Yes, thank you to Apple Bank. Thank you to Jefferson and Christopher for this wonderful program today. It was such valuable information. Like I said, I will email you the slideshow if you registered for this program. We wanted to thank everyone at Apple Bank who helped us to get this program together.
Thank you to Samantha Dodds and Judy Vigo at Brooklyn Public Library for helping me out and thank you to you all who made the effort to show up on this nice spring day to hear this valuable information. So, I would like to say thank you and have a good afternoon. Thank you, Apple Bank, and we will see you all later. Have a great afternoon.