BE SCAM SMART

OPERATION S.A.F.E.

STOP ADULT FINANCIAL EXPLOITATION

DEPARTMENT OF FINANCIAL SERVICES
STATE OF FLORIDA

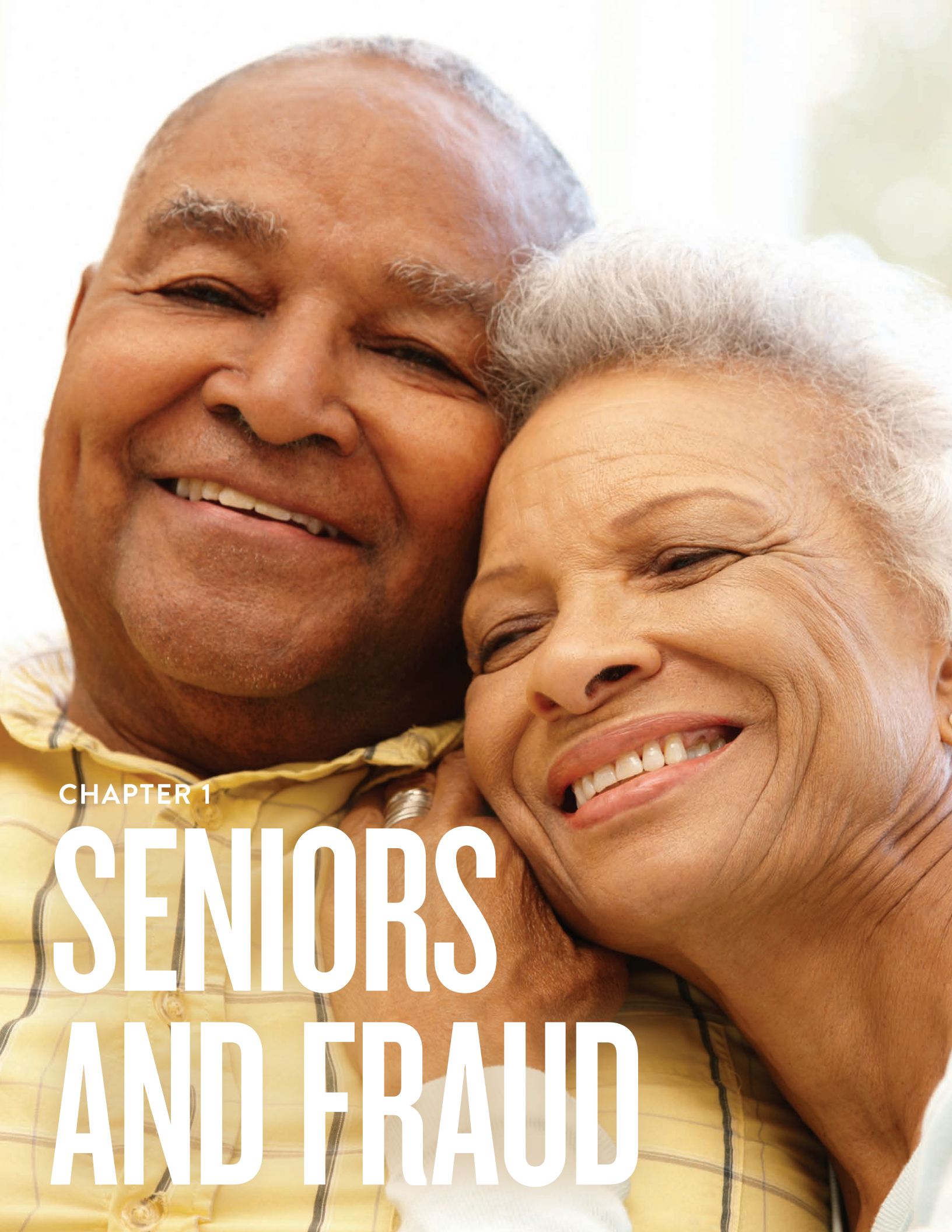
OPERATION S.A.F.E.

BE SCAM SMART

Financial education is important. The key to protecting yourself from becoming the victim of consumer fraud, scams and identity theft is awareness. Having a full understanding of your financial information will not only help you make suitable investment decisions, it will also help you protect yourself from fraud and recover from it, if it unfortunately occurs.

Remember the three P's – **Protect, Prevent and Police.** Protect your personal information, prevent yourself from becoming a victim and police your personal information by contacting financial institutions and credit card companies immediately if a problem is detected.

CONTENTS

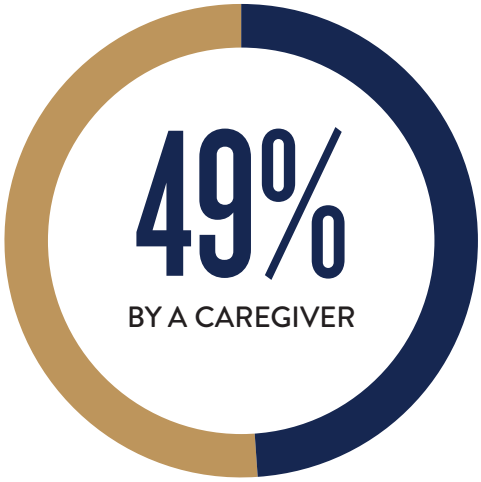


CHAPTER 1

SENIORS AND FRAUD

Seniors control a majority of the nation's wealth, which is one of the main reasons that seniors are a target for financial exploitation. Sadly, it isn't always the dishonest salesperson or scam artist that may be thinking about trying to take advantage of you financially.

One out of every five adults age 65 and older has been the victim of a financial scam:



Everyone is susceptible to fraud. However, seniors are targeted more frequently because they have a "nest egg," usually own their own home and have excellent credit. Seniors are also generally more polite and trusting than younger generations.

Scam artists have also realized that seniors can be reluctant to report fraud for a few reasons:

- Seniors are not sure where to report fraud.
- Seniors may not want their family members to think they are no longer able to handle their own financial affairs.
- Scam artists believe seniors make poor witnesses. They don't think seniors will be able to remember the details.

There are behaviors that seniors are more likely to exhibit than others that can result in becoming the victim of fraud. Below are a few tips to reduce the risk of becoming a fraud victim.

- Be wary of someone who tries to incorporate him or herself into your personal life by developing a parent/child or dependency relationship with you. Resist offers to allow them to take you to a medical appointment, grocery shopping or a special event.
- Never sign any document containing blanks and before you sign a contract, conduct a thorough review of the terms. Make sure all sections are properly completed.
- Do not allow yourself to be rushed through the process. If the agent or salesperson is urging you to make a quick decision, end the conversation. Let them know you are not going to make an investment or financial decision without first taking the time to consider your options.
- If it sounds too good to be true, it probably is. Exercise due diligence and verify before you buy.

Back to Table of Contents

CHAPTER 2

PSYCHOLOGY OF A SCAM

Scam artists are masters of persuasion who make a living by preying on seniors and flaunting offers that sound both good and true. These scam artists will often start their ploy by asking general but somewhat personal questions to gain insight regarding your family, occupation, hobbies and finances. Listed below are some of the most common tactics used by scam artists:

PHANTOM RICHES

The scam artist will dangle the prospect of wealth, perhaps a guaranteed monthly income, if you purchase a certain product.

SOURCE CREDIBILITY

The scam artist will make it appear that his or her company is reputable or that they have special credentials or experience. The scam artist might say something like "trust me, as the Vice President of Sales at XYZ Firm, I would never sell you an investment that doesn't produce."

SOCIAL CONSENSUS

The scam artist will want you to believe that people you may know have already invested or purchased the product, such as your neighbors, high-ranking church officials or well-known community leaders.

FALSE AFFILIATION

Similar to source credibility, the scam artist claims to work for a company with a name that gives the appearance that it's a part of or affiliated with a senior advocacy group, such as AARP®, or a government agency, to gain your trust.

SENSE OF URGENCY

The scam artist will try to get you to buy now by saying the offer is only extended to the next 10 people who purchase today.

These tactics probably sound familiar and it is possible that they are used by legitimate marketers as well. The big difference is that if the deal being offered is legitimate, it will still be there tomorrow. Take time to think and consider all factors before making a financial decision.

CHAPTER 3

SENIOR FRAUD & SCAMS

There are hundreds of scams that take place daily. Listed below are some of the more common fraud and scams that are directed at seniors along with tips on how to avoid falling victim to these scams.

GRANDPARENT SCAM

- The grandparent scam takes place by phone.
- The imposter pretends to be a grandchild and says something similar to – 'Hi Grandpa, it's your grandson and I'm in trouble.' Prompting you to say 'John, is that you?' The caller will confirm the identity of the grandchild – 'Yes Grandpa, this is John,' and then ask that you purchase a prepaid debit card, such as a Green Dot® card, or wire the money via Western Union® or MoneyGram®, but tell you not to mention the request to his parents.
- The scam artist may even go as far as giving reasons why they sound different, claiming to have a broken nose from an altercation or other ailment.

This scam tugs at the heartstrings, but what the scam artist really wants is the money in your wallet. You can avoid getting caught in this scam by not mentioning the name of your grandchild to an unknown caller and doing some research.

If you are tempted to wire money as the caller requested, first verify that your grandchild is traveling and away from home by contacting his or her parents. You may even want to contact your grandchild directly. Otherwise, once the money is wired, it is gone for good.

LOTTERY AND SWEEPSTAKES FRAUD

- Prize and sweepstakes fraud is extremely prevalent among seniors.
- This type of fraud can be initiated in person, by phone, email or mail.
- The scam artist will inform you that you have won a prize or the lottery, often from another country, but before the prize or winnings can be claimed, a fee must be paid for taxes, shipping and handling or other fees.

Do not participate in these types of offers. The Federal Trade Commission receives thousands of complaints every year regarding this type of fraud. Legitimate sweepstakes don't require payment or the purchase of a product to enter or improve chances of winning, or to pay 'taxes' or 'shipping and handling charges' to receive the prize. Taxes and fees are deducted from the lottery winnings prior to the winner receiving it.

INVESTMENT SCAMS

Investment scams are those scams that are designed to take advantage of seniors who are at or near retirement and are interested in safeguarding cash for their later years. Two of the more common investment scams are Ponzi and pyramid schemes.

- Ponzi schemes promise high financial returns or dividends that are not available through traditional investments. Initial investors are paid 'dividends' as other investors sign on. Payments continue until a sufficient number of new investors cannot be found to continue the scheme or the administrator flees with the money.
- Pyramid schemes are similar to Ponzi schemes, but with a critical difference. The victims of the fraud are encouraged to recruit additional investors (victims) through the payment of recruitment commissions and fees.

You can avoid getting caught up in these types of schemes by consulting an unbiased third-party, such as an unconnected, licensed financial advisor, before investing and by researching the company and 'agent.'

You can verify the license of a broker or financial advisor with the Florida Office of Financial Regulation at **FLOFR.gov**. Remember, if it sounds too good to be true, it probably is!

REVERSE MORTGAGE SCAMS

Reverse mortgages are legitimate products and can be a good financial option, but you want to make sure you understand all of the terms. Reverse mortgage scams are engineered by scam artists to steal the equity from the property of unsuspecting seniors or to use seniors to unwittingly aid in stealing equity from a flipped property. To avoid getting involved in a reverse mortgage scam:

- Do not respond to unsolicited advertisements.
- Do not sign documents regarding a reverse mortgage that you do not fully understand.
- Be suspicious of anyone claiming that you can own a home with no down payment.
- Do not accept payment from individuals for a home you did not purchase.

If you are interested in a reverse mortgage, seek out your own reverse mortgage counselor.

ROMANCE SCAM

The romance scam takes place on the internet through online dating websites or social media sites.

- A scam artist pretends to have romantic intentions towards you to gain your affection and trust, often claiming to be from another country.
- The scam artist will then begin asking for money, perhaps for a ticket to travel to visit you, medical/education expenses, or to pay bills such as internet and phone to continue the relationship.

HOME IMPROVEMENT SCAMS

Look out for home improvement contractors who leave your home in worse shape than they found it. They usually knock on your door with a story or a deal – the roofer who can spot some missing shingles on your roof or the paver with some leftover asphalt who can give you a great deal on driveway resealing.

The scam artist will offer to do the work now in exchange for an assignment of benefits on your insurance policy, meaning once the claim is finalized through your insurance company, the check will be provided directly to the contractor or handyman rather than you.

There are several reasons you should not enter into this type of agreement.

- The claim check may exceed the actual cost of the repairs made to your home and the work may be completed with inferior products.
- You may be exposing yourself to other types of theft, such as workers requesting to enter your home to get a drink of water or use the restroom and stealing money or valuables in the process.

You can avoid becoming the victim of a home improvement scam by:

- Checking out the company with the Better Business Bureau.
- Collecting copies of the contractor's license and contractor number for your records and verifying with the Florida Department of Business and Professional Regulation at **(850) 487-1395** or by visiting **MyFloridaLicense.com/DBPR/**.

- The scam artist preys on a person's need for companionship and their intentions to help someone out in a time of crisis. Some will not actually go as far as to ask for money. Rather, they will simply share their heartbreaking situation with you in hopes that you might offer to send them money.

To avoid falling for this type of scam, never send money to someone you do not truly know and do not disclose personal information online.

TELEMARKETING FRAUD

Telemarketing fraud is very common among the senior population because this demographic is twice as likely to make purchases over the telephone. Scam artists target individuals age 60 and older, and try to peddle bogus products and services, with high pressure techniques designed to keep the senior talking. The scam artist will try to entice you with 'free' prizes, low-cost vacations or medical and health care products. It is very difficult to get your money back when you have been scammed over the phone. Be wary of callers trying to get you to purchase products or services over the phone and if you hear any of the following or similar phrases say 'No, thank you' and hang up:

- 'You must act now or the offer won't be good.' – If the offer is legitimate, it will still be good tomorrow. Don't allow yourself to be pressured into making a decision on the spot.
- 'You've won a free gift, vacation or prize, but a fee is required for postage and handling or other charges.' – It's not free if a fee is required.
- 'You can't afford to miss this high-profit, no-risk offer.' – There is no such thing as a risk-free offer.

- Verifying with the Department's Division of Workers' Compensation that the contractor has workers' compensation coverage. If they don't, you could be liable for any injuries. You can verify with the Division of Workers' Compensation at **(850) 413-1609** or by visiting **MyFloridaCFO.com/Division/WC/**.

Below are additional scams to be aware of:

- A plumber who advises you that your entire plumbing system should be replaced due to a leaky faucet, turning a small job into a large costly project.

- A roofer who advises you that your entire roof needs to be replaced due to a minor leak.

To decrease the number of telemarketing calls you receive, add your telephone number(s) to the Florida Do Not Call List at **1-800-435-7352** or online at **FDACS.gov/Consumer-Resources/Florida-Do-Not-Call**.

You may also add your telephone number(s) to the Federal Trade Commission's National Do Not Call Registry at **1-888-382-1222** or by visiting **DoNotCall.gov**.

CHARITABLE DONATION SCAMS

Charitable donation scams are most popular after a disaster or devastating event has occurred. Scam artists will prey on the generosity of seniors and may contact you by phone or in person and ask for a charitable donation for a specific cause.

To avoid falling for this type of scam, only donate to local and familiar charities. The Department of Agriculture and Consumer Services maintains a list of registered charities in Florida. To determine if a charity is registered visit **FDACS.gov/** and use the **Check-A-Charity** tool.

IRS IMPOSTER SCAM

Scam artists are aware that no one wants to be audited by the IRS and are preying on seniors' fears. A scam artist contacts you by phone claiming to be an IRS agent. The scam artist will provide a false name, badge number and even share personal information they found about you from the internet, to increase their credibility. The IRS imposter informs you that you are being contacted because of an outstanding tax debt and you must pay the debt by a Green Dot® or MoneyPak® prepaid card or wire the money via Western Union® or MoneyGram® to settle the debt. The imposter claims that if payment is not received immediately you will be arrested or a lien will be placed on your home. Remember, the IRS will not threaten to arrest consumers to pay a debt, as it has legal methods to accomplish that, such as wage garnishment.

The IRS does not use email, text message or any social media to discuss your personal tax issues involving bills or refunds. The IRS has begun utilizing the services of private collection agencies (PCA) but will contact the taxpayer through the mail before they receive a phone call about any tax debt. Also, the IRS will allow you to appeal and correct any error on tax documents.

TAX IDENTITY THEFT SCAM

Each year you may look forward to filing your tax return in hopes of receiving a refund to assist

TECH SUPPORT SCAM

Scam artists set up fake websites, offer free "security" scans and send frightening messages to try to convince you that your computer is unprotected and infected. They will also try to sell software to fix your computer. Either the software doesn't work or, worse, it could be malicious software (malware) that has the single purpose of stealing your personal information.

The scam sometimes starts with a phone call from an imposter who claims to represent a legitimate tech support company and shares basic information that can be obtained from public directories. The scam artist may use technical jargon to confuse and frighten you to grant them access to your computer remotely. Once the scam artist has access to your computer, they can obtain all of the personal information you have stored.

Also, clicking on "pop-up" ads can allow scam artists access to your computer. Scam artists will place online ads to convince you to call or email them. They pay to boost their ranking in search results, so their websites and phone numbers appear above those of legitimate companies. Often while searching online, you might accidently pick up a Trojan, a type of malware that sneaks into your computer undetected. The Trojan will place fake pop-up messages on your computer indicating there is something wrong with your system and ask you to call the scammer for help.

with paying debt or adding to your savings and emergency fund. Identity thieves have the same goal but do so at your expense.

The tax identity theft scam is a version of the IRS scam in which the scam artist uses your personal information to file a false tax return and collect your refund. All that is needed to perpetrate this scam is your name, Social Security number, date of birth and a fraudulent W-2 form, which the scam artist can easily create. Most victims are not aware of the fraud until they attempt to file their own tax return.

To reduce the risk of becoming a victim of the tax identity theft scam:

- File your taxes early, even if you don't have any income, believe your income is below the minimum required to file, are self-employed or receive government benefits such as Social Security. This decreases the amount of time an identity thief has to file a return in your name.

- Get an **Identity Protection Personal Identification Number** (IP PIN) from the IRS. An IRS IP PIN is a 6-digit number that is assigned annually. The IP PIN acts as an authentication number to validate the correct owner of the Social Security number listed on the tax return being filed. The fastest way to get an IP PIN is to use the online **Get an IP PIN** tool. An identity verification process is required. An IP PIN is valid for one calendar year, and a new one is generated each year.

- To check the status of your refund, visit **Where's My Refund?** at **IRS.gov/Refunds**.

- Use the IRS's **Free File** program and take advantage of Volunteer Income Tax Assistance **(VITA)**, a free tax preparation organization.

If you become a victim:

- File a 14039 form with the IRS. This form is used to report identity theft to the IRS. The IRS will use the form to document situations where individuals are or may be victims of identity theft.

- Report identity theft to the Federal Trade Commission at IdentityTheft.gov and also to your local police department. For more information read this **Identity Theft Brochure**.

Do not rely on caller ID alone to authenticate a caller, as scam artists may spoof the phone number or organization to make it appear as if they're legitimate. Spoofing technology makes it easy for scam artists to disguise the actual telephone number, company and location they are calling from. Never provide your credit card or financial information to someone who calls and claims to be from technical support. Never share your password over the phone. No legitimate organization calls you unsolicited and asks for your password or personal information. If a caller pressures you to buy a computer security product or says there is a subscription fee associated with the call, hang up. If you're concerned about your computer, call your security software or computer company directly and ask for help. You may also visit the support webpage of the companies for assistance.

- Consider placing a security freeze on your credit report, which prevents any new lines of credit accounts from being opened in your name. The Fair Credit Reporting Act allows consumers to place a security freeze on their credit report free of charge. You will need to request the security freeze with each of the three credit bureaus and can do so online, by phone or by mail. A security freeze can be lifted temporarily or removed at any time by contacting each of the three credit bureaus. This is the most secure way to protect your credit.

For more information, visit **IRS.gov** and **Consumer.FTC.gov**.

JURY DUTY SCAM

Chances are you have received a jury summons to report to jury duty at some point. If you do, it is your civic duty and should not be taken lightly. However, scam artists will try to use fear of missing jury duty to scam you.

In this scam, you will typically receive a phone call from a "law enforcement officer" or "court official" claiming that you have missed jury duty and are now facing serious penalty fees that must be paid immediately or you will be arrested. The scam artist may ask for your personal information for verification purposes. Once the scam artist has convinced you of your "delinquency," they will demand payment in the form of a wire transfer, Green Dot® or MoneyPak® prepaid card, gift card or ask for your bank account number. Don't provide the requested payment and hang up.

The court will never contact you via phone or email regarding a missed jury duty summons. Instead, you will receive written correspondence by mail. The court will also never demand your personal information or immediate payment over the phone. If you are truly concerned that you may have overlooked a jury summons, look up the phone number for the Clerk of Courts in your county and call directly.

Additionally, as a senior, you may be excused from jury duty. Contact your local Clerk of Courts to determine if your appearance can be waived.

ADVANCE FEE LOAN

Scam artists are continually developing new versions of the advance fee scam. They are

ONLINE PHISHING SCAM

Scam artists attempt to grab your attention with the phishing scam. You may receive an email claiming to be from your financial institution or credit card company. The email states that during a review of your account, the company was not able to verify your information. You are asked to click on a link embedded in the email to update and verify your personal information. The email may look authentic but can redirect you to a site that downloads malware on your computer to search for sensitive data.

You can protect yourself from this scam by not clicking on any links in an email that claims to be from your financial institution or credit card company asking for your personal financial information. If you believe the email may be legitimate, contact your financial institution or credit card company at the telephone number that is listed on your statement or back of your credit card.

aware that many seniors are on a fixed income and will use the possibility of an advanced fee loan to scam them. The scam artist guarantees that you will receive a loan regardless of your credit history, but you will have to pay a fee upfront. Unfortunately, you receive little or nothing in return. If you receive the loan, the interest rate may be exorbitant and difficult to repay, which puts you in a cycle of debt. Remember, a legitimate lender will never guarantee or say that you will be approved for a loan or credit card before you apply, especially if you have had credit issues in the past. Additionally, you should not have to pay a fee upfront prior to receiving a loan.

To avoid falling victim to this scam, make sure you clearly understand the terms of any agreement before signing. Check with your local bank or credit union to determine your loan options. Remember, if it sounds too good to be true, it probably is.

FAKE CHECK OR MONEY ORDER SCAM

This scam targets consumers who are selling or buying items through sites like Craigslist®, eBay®, or Facebook® and classified ads. The scam artist will reply to your offer to sell an item but pay with a check or money order that may be illegitimate and usually for more than the cost of the item you're selling. After you have deposited the fake check or money order into your account, the scam artist will request that you return the overpayment amount via mail or Western Union®, MoneyGram®, a cashier's check or money order. You find out later that the check or money order is fake. Since you deposited the check into your account, you are responsible for the amount of the fake check and you have lost the money that you "returned" to the scam artist.

No matter how tempting the scam artist's offer is or how convincing the story, do not accept payment for more than it was advertised. Ask the buyer to write the check or money order for the exact amount of the item. If they refuse, chances are it's a scam! Please also verify the funds in the checking account before you deposit it into your account. You may do so by calling the issuing financial institution and requesting the verification.

FAKE DEBT COLLECTOR SCAM

Sometimes it can be hard to tell the difference between a legitimate debt collector and a fake one. Sometimes fake debt collectors may even have some of your personal financial information, such as your bank account number.

The scam artist poses as a representative from a debt collection agency or attorney demanding immediate payment of delinquent loans or a loan you may have received but for amounts you do not owe. The imposter may threaten you with wage garnishment, lawsuits or arrest if you do not pay. Scam artists will often use spoofing to make it appear as if they're calling from a legitimate debt collection agency. The scam artist may request that the payment be made via wire transfer (Western Union®, MoneyGram®, etc.), pre-paid debit card (Green Dot® or MoneyPak®) or with a gift card.

To avoid becoming a victim of the fake debt collector scam, ask the scam artist for their name, company, street address and telephone number. Inform the scam artist that you will not discuss the debt until you receive a written validation notice. Advise them that the notice must include the amount of the debt, the name of the creditor you owe and your rights under the federal Fair Debt Collection Practices Act. If the scam artist refuses to provide you all or any of this information, do not hesitate to hang up and do not pay! Paying a fake debt collector will not make them end the harassing calls; they may make up another debt to try to obtain more of your money.

> "If it sounds too good to be true, it probably is."

CHAPTER 4

10 WAYS TO AVOID FRAUD & SCAMS

Scam artists are always changing their scams and coming up with new tricks. If something doesn't feel right about an email, phone call or in-person situation, don't override your gut instinct, it is usually right! Always be cautious, investigate and use these tips to avoid fraud and scams:

1. SPOT IMPOSTERS. Scam artists often pretend to be someone you trust, like a government official, a family member, a charity or a company you do business with. Don't send money or give out personal information in response to an unexpected request – whether it comes as a text, a phone call or an email. If you feel the request may be legitimate, contact the person or organization directly through a different form of communication.

2. DO ONLINE RESEARCH. Before doing business with an unfamiliar company, type the company or product name into your favorite search engine with words like "review", "complaint" or "scam." Or search for a phrase that describes your situation, such as "technical support call." You can even search for phone numbers to see if other people have reported them as scams.

3. DON'T BELIEVE YOUR CALLER ID. Scam artists use spoofing technology to fake caller ID information, so the name and number you see aren't always real. If someone calls asking for money or personal information, hang up. If you feel the request may be legitimate, contact the organization via telephone or email directly, with information you found on their website.

4. NEVER PAY UPFRONT FOR A PROMISE. Someone might ask you to pay in advance for things like debt relief, credit and loan offers or even a job. They might say you've won a prize, but first you must pay taxes or fees. If you do, they will probably take the money and disappear.

5. CONSIDER YOUR PAYMENT METHOD. Credit cards have significant fraud protection built in, but some payment methods don't. Wiring money through services like Western Union® or MoneyGram® or using prepaid debit cards like Green Dot® cards is risky because it's nearly impossible to get your money back. Government offices and honest companies will not require you to use these payment methods. Also, if you're asked to pay by money transfer, Bitcoin or a gift card, it is likely a scam.

6. TALK TO SOMEONE. Before you give up money or personal information, talk to someone you trust. Con artists want you to make decisions in a hurry. They might even threaten you. Slow down, analyze the story, do an online search and consult an expert or even talk to a friend. Talking over the scenario may help you see more clearly if sending money or personal information is in your best interest.

7. HANG UP ON ROBOCALLS. If you answer the phone and hear a recorded sales pitch, hang up and report it to the FTC at **ReportFraud.FTC.gov** or call **1-877-FTC-HELP** (**1-877-382-4357**). These calls are illegal and often the products are not legitimate. Don't press "1" to speak to a person or to be taken off the list. That could lead to more calls. Block unwanted calls and text messages.

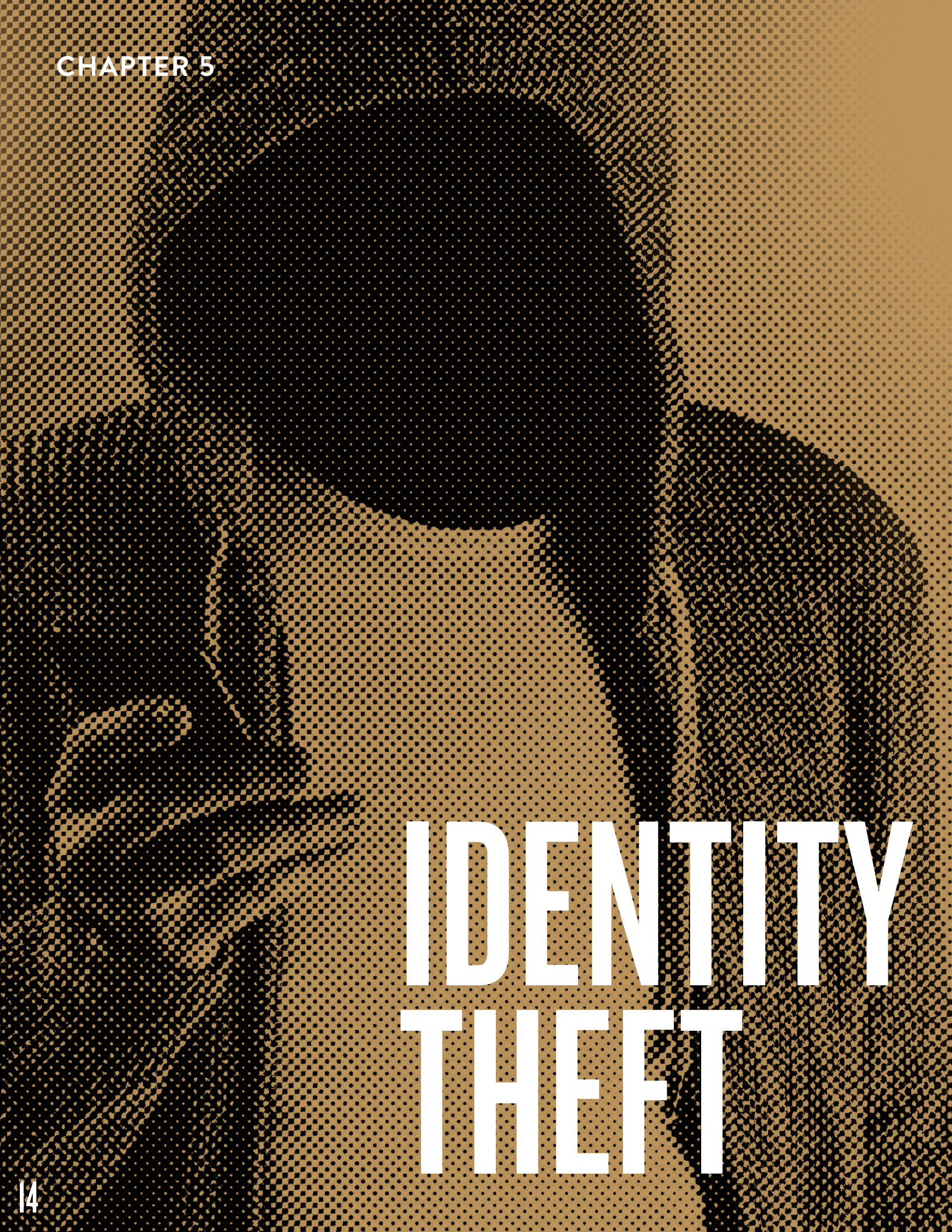
8. BE SKEPTICAL ABOUT FREE TRIAL OFFERS. Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and always read the cancellation policy. Be sure to check your monthly financial statements for charges you don't recognize as well.

9. DON'T DEPOSIT A CHECK AND WIRE MONEY BACK. Any time someone offers or gives you too much money and asks you to return the difference, beware. By law, banks must make funds from deposited checks available within days but uncovering a fake check may take weeks. If a check you deposit turns out to be a fake, you're responsible for repaying the bank.

10. SIGN UP FOR FREE SCAM ALERTS. The Florida Department of Financial Services and Federal Trade Commission both offer free email alerts with the latest tips and advice on current scams.

a. To sign up for the Department of Financial Services Consumer Alert email service, go to **MyFloridaCFO.com/Division/Consumers/Alerts**.
b. The FTC Consumer Alert email sign-up is on their website at **FTC.gov/scams**. By staying informed, you can protect yourself from fraud and scams.

CHAPTER 5



IDENTITY THEFT

Identity theft is the fraudulent use of your personal information and Florida ranks as one of the top three states for this crime. Identity theft can occur in many forms such as in person, by phone, email or via the internet. Unfortunately, identity thieves often target seniors, so it is important to stay on guard when someone contacts you seeking personal or financial information.

PROTECT. PREVENT. POLICE.

STEP 1: Protect Your Personal Information.

Your first line of defense is to protect your personal information.

- Use PINs and passwords for your accounts that will be easy for you to remember but difficult for others to guess. Don't use words that can be found in any dictionary, in any language. You should also avoid using your year of birth as a PIN or the month and day of your birthday. These are some of the first numbers an identity thief will try. When entering your PIN at a store or gas pump, cover the keypad. Identity thieves will look over your shoulder or set up cameras at gas pumps to record the pin number you enter.
- For online passwords, use a minimum of 8-12 upper and lower-case characters, numbers and with at least one symbol such as an ampersand (&) or percent sign (%). Each character you add makes it harder for a password cracking tool to figure out.
- Be creative and change your password regularly. You should also avoid using the same password for multiple accounts.
- If you have a mobile phone, consider activating two-factor authentication for a website or service if it is available. Each time you sign into your account you will be required to enter your username and password and the company will send you a numerical code via text message. You will only be able to successfully login with all three pieces of information, preventing a scam artist from gaining access to your account with just a username and password.
- Ask salespeople and others, if information such as a Social Security or driver's license number is necessary or if they can verify your identity using the last 4 digits instead. A telephone number should suffice when you are writing a check in a store. If someone does require your Social Security number, ask for information about its privacy policy and ensure that it has security measures in place.
- Don't overshare on social networking sites. Identity thieves can find information about your life and use it to answer security questions on your accounts which may give them access to your money and personal information.

STEP 2: Prevent Yourself From Becoming A Victim.

The second line of defense is to prevent yourself from becoming a victim.

- Shred all personal and financial documents before throwing them away. If you are shredding your personal documents, you won't be providing dumpster divers with anything but confetti and rotten food.
- Destroy the labels on your prescription bottles before you recycle or throw them out.
- Before you dispose of a computer, use a wipe utility program to overwrite the hard drive. Before disposing of any personal devices, like mobile phones or tablets, check the manual or the manufacturer's website for information on how to transfer your information to a new device and then delete that information from the old device permanently.
- Do not provide your credit card number, password or PIN over the phone or internet to someone who has contacted you to 'verify'

information. If you receive this type of request via phone or email, immediately contact your credit card company or financial institution using the number on your statement or on the back of your debit or credit card.

- Do not share your passwords, PINs or access codes with family members or friends. If you must write your passwords down on paper, make sure you store it a secure location away from your computer and keep it secured from people who come into your home.
- Contact your local post office and place a hold on your mail if you are going to be away for an extended period. This will decrease the chance of someone obtaining your personal information from your mail.
- When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.
- Take outgoing mail to the post office collection boxes or the post office. Don't use the flag to signal to everyone that you have mail to be picked up. Pick up your mail from the mailbox promptly.
- Consider opting out of prescreened offers of credit and insurance by mail. You can opt-out for five years or permanently. To opt-out call **1-888-567-8688** or go to **OptOutPrescreen.com.** (By opting out, you may miss out on some offers for new credit.)
- Limit what identification, credit and debit cards you carry with you. Only carry what you need that day, leave the rest at home. Never carry your Social Security card with you.
- Start an identity theft file. Set up a folder and put in it your credit reports, security freeze documents, copies of annual privacy notices and any potential evidence, such as mail to your address that is in someone else's name. Also, make a copy of the contents of your wallet. Include the front and back of your driver's license, credit cards, club memberships, etc. Keep this folder in a secure location.

STEP 3: Police Your Personal Information.

The third line of defense against identity theft is to police your personal information.

- Check your financial statements monthly for errors or erroneous charges. If you see unauthorized charges, contact your financial institution immediately.
- Request and review your credit report. You can request a free credit report from each credit reporting agency from **AnnualCreditReport.com** or by calling **1-877-322-8228**. **AnnualCreditReport.com** is the only source for free credit reports authorized by Federal Law.

NOTE: Each of the three credit reporting agencies, Equifax, TransUnion and Experian are required to provide you a free credit report every twelve months, at your request. Due to various breaches, you may be able to access your credit report online with more frequency. If you request your report online, you will be asked some hard question only you know, to ensure only you can access your credit information. You may need to have your records on hand to answer these questions.

What To Do If You Become A Victim Of Identify Theft?

If you discover you have been a victim of identity theft, take the following steps:

- Contact the fraud department of the companies where you know the fraud has occurred and ask them to close or freeze those accounts, to help prevent new charges from being added.
- Contact one of the three credit reporting agencies – Equifax, Experian or TransUnion and place a free, one-year fraud alert on your credit report. A fraud alert will make it difficult for someone to obtain credit in your name because it tells creditors to follow certain procedures to protect you. As soon as one of the credit reporting agencies processes your fraud alert, it will notify the other two, which then must also

place fraud alerts in your file. A fraud alert will remain on your credit report for one year unless you request it be removed. You may also request an extended fraud alert that stays on your credit report for 7 years.

- Request a security freeze on your credit report to prevent third parties from receiving a copy of your credit report without your approval. The Fair Credit Reporting Act allows consumers to place a security freeze on their credit report free of charge. You will need to request the security freeze with each of the three credit bureaus and can do so online, by phone or by mail. A security freeze will not affect any current lines of credit you have open, it will only prevent new lines of credit from being open.

  A security freeze can be temporarily lifted for a period of time or removed altogether. To request a temporary lift or to remove a security freeze, you will have to contact each of the three credit bureaus. If you request a temporary lift online or by phone, a credit bureau must lift a freeze within one hour. By mail, it may take up to three business days after receiving your request.

  NOTE: After receiving your freeze request, each bureau will provide you with a unique personal identification number (PIN) or password. You will need this PIN or password to lift the freeze by phone or mail.

- Report identity theft to the Federal Trade Commission (FTC) and create an Identitv Theft Report at **IdentityTheft.gov**.An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft and help get information about accounts that a thief opened in your name.

  To create an Identity Theft Report:

  - Go to **IdentityTheft.gov** and follow the steps to report identity theft and get a recovery plan that you will be able to print out. You can update your plan as needed and track your progress.

  - File a police report in the local jurisdiction where the identity theft occurred. Take your FTC identity theft report with a photo ID, proof of address and any other proof of the identity theft you have. If the crime occurred somewhere other than where you live, you may wish to report it to the law enforcement agency in that jurisdiction as well. Be sure to obtain a copy of the police report and/or report number for your file.

  - File a complaint with the Federal Trade Commission (FTC) at **ReportFraud.ftc.gov** or call **1-877-438-4338**; TTY: Your completed complaint is called an FTC Affidavit.

  - File the Identity Theft Report with each of the three credit reporting agencies.

SHRED PERSONAL INFORMATION

CHAPTER 6

ANNUITIES & REVERSE MORTGAGES

ANNUITIES

An annuity is a contract or agreement with an insurance or investment company that provides a source of income or a series of payments from an investment, either now or at a set future date, such as retirement. An annuity is a longterm investment tool and would not be the appropriate product if you are seeking a short term investment opportunity.

Make sure you fully understand the surrender period and the associated fees before you decide to purchase an annuity. Before entering into an annuity contract, take the time to carefully consider your immediate and future financial needs. This will assist you in determining if the product is a suitable investment for you.

First ensure the agent has a valid license with the Department of Financial Services by visiting our licensee search page at **https://licenseesearch.fldfs.com** or calling **1-877-MY-FL CFO.** Unlicensed individuals have not demonstrated and proven to the Department that they have the required knowledge and skills to sell annuities.

Before signing an annuity contract, ask your agent or insurance company these questions:

- What is the guaranteed minimum interest rate?
- Are there additional charges included in the premium?
- What are the surrender charges or penalties if I withdraw some or all of my money early and how many years will I be subject to those charges?
- Can I make partial withdrawals without penalties or losing interest?
- Does my annuity waive surrender charges if I am confined to a nursing home or diagnosed with a terminal illness?
- What are my income options when my annuity reaches its maturity date?
- What is my death benefit?
- Can the annuity or interest decrease in value?
- What is the free look period?
- What is the length of the contract?
- What is your commission?

REVERSE MORTGAGES

A reverse mortgage is a loan for seniors or retirees designed to allow the use of home equity for financial security, while retaining ownership. A reverse mortgage turns a portion of home equity into regular cash payments for the homeowner. It is similar to a traditional mortgage, but in reverse. Rather than making a payment to the lender each month, the lender makes payments to the borrower(s) or homeowner(s) through advances against the home's equity.

As with any financial product, carefully review the terms and conditions of a reverse mortgage. If there is language in the contract that is ambiguous or confusing, talk to the agent and/or company offering the reverse mortgage for an explanation and additional information.

Here are some questions you should ask your agent or reverse mortgage company:

- What types of homes are acceptable for a reverse mortgage?
- When the loan is due, is it possible for me to owe more than the home is worth?
- What kinds of fees are involved?
- Are reverse mortgage interest rates fixed or variable?
- By accepting a reverse mortgage, am I giving my home to the bank?
- Will I have to pay taxes on the money I receive?
- Will I have to move out of my home if I outlive the loan?
- What happens if I pass away while living in the home?
- Will I be able to leave the home to my heirs?
- Does the reverse mortgage affect my eligibility for Social Security or other government assistance?
- Will I be required to purchase homeowner's insurance for my home?

APPENDIX

DEPARTMENT OF FINANCIAL SERVICES

The Department serves consumers and taxpayers through the work in its various Divisions, as well as additional initiatives set forth by the Chief Financial Officer of Florida. The Department provides information and services on issues ranging from insurance education and assistance, insurance fraud, fire prevention and safety, and even unclaimed cash and property. Our top priority is to protect your hard-earned dollars and keep them in your pocket where they belong.

DIVISION OF ACCOUNTING AND AUDITING

The Division of Accounting and Auditing ensures that Florida taxpayers' dollars are spent responsibly by reviewing the agreements that provide goods and services to the state and approving payment requests. For additional information, contact the Division of Accounting and Auditing at **(850) 413-5510** or visit **MyFloridaCFO.com/Division/AA/**.

DIVISION OF CONSUMER SERVICES

The Division of Consumer Services assists consumers with resolving insurance complaints and making informed insurance and financial decisions. You can reach Consumer Services toll-free by dialing **1-877-MY-FL-CFO (1-877-693-5236)** or from out of state by calling **(850) 413-3089.** You may also visit **MyFloridaCFO.com/Division/Consumers**.

DIVISION OF FUNERAL, CEMETERY AND CONSUMER SERVICES

The Division of Funeral, Cemetery and Consumer Services provides assistance to purchasers of pre-need burial rights; funeral or burial merchandise; or funeral or burial services. For additional information, contact the Division of Funeral, Cemetery and Consumer Services toll-free by dialing **1-800-323-2627** or from out of state by calling **(850) 413-3039.** You may also visit **MyFloridaCFO.com/Division/FuneralCemetery/**.

DIVISION OF INSURANCE AGENT AND AGENCY SERVICES

The Division of Insurance Agent and Agency Services provides assistance related to the licensing of agents and agencies to sell insurance and investigates alleged violations of the Florida Insurance Code and Administrative Rules. To **verify a license** or report a violation call the Licensing Hotline at **(850) 413-3137.** For more information, visit **MyFloridaCFO.com/Division/Agents/**.

DIVISION OF INVESTIGATIVE AND FORENSIC SERVICES

The Division of Investigative and Forensic Services serves and safeguards Florida's citizens and businesses against acts of insurance fraud, arson, workers' compensation fraud, financial crime and provides forensic services for law enforcement. If you or someone you know has been a victim of insurance fraud call the DFS Fraud Hotline at 1-800-378-0445 or visit the Report Suspected Fraud website at **First.FLDFS.com**. To report suspected arson, call the Arson Tip Hotline at **1-877-NO-ARSON (1-877-662-7766).**

DIVISION OF PUBLIC ASSISTANCE FRAUD

The Division of Public Assistance Fraud safeguards Floridians against public assistance fraud and the impact of these crimes by enforcing state laws regarding program eligibility and proper use of public assistance benefits. To report suspected public assistance fraud, call the Fraud Hotline at **1-866-762-2237** or visit the Report Suspected Fraud website at **MyFloridaCFO.com/Division/PAF/Report-Fraud.**

DIVISION OF REHABILITATION AND LIQUIDATION

The Department of Financial Services serves as the Receiver of any insurer placed into receivership in Florida. The Division of Rehabilitation and Liquidation plans, coordinates and directs the receivership processes on behalf of the Department. For additional information related to companies in receivership call toll-free at **1-800-882-3054** or out of state **(850) 413-3132.** You may also visit **MyFloridaCFO.com/Division/Receiver**.

DIVISION OF RISK MANAGEMENT

The Division of Risk Management is responsible for the management of claims reported by or against state agencies and universities for coverage under the State Risk Management Trust Fund. For additional information, contact the Division of Risk Management at **(850) 413-3120** or visit **MyFloridaCFO.com/Division/Risk/**.

DIVISION OF STATE FIRE MARSHAL

The state's CFO also serves as Florida's State Fire Marshal. The Division of State Fire Marshal provides assistance related to fire prevention and enforcement. For more information, visit **MyFloridaCFO.com/Division/SFM/**.

DIVISION OF TREASURY

The Division of Treasury is responsible for ensuring that cash and other assets held for safekeeping within the Treasury are accurately accounted for, effectively invested and competently protected. For additional information, contact the Division of Treasury by calling **(850) 413-3165** or by visiting **MyFloridaCFO.com/Division/Treasury/**.

DIVISION OF UNCLAIMED PROPERTY

The Division of Unclaimed Property holds funds from dormant accounts, such as utility companies, as well as tangible property such as jewelry and coins. To find out if the state is holding property that belongs to you or someone you know, contact Unclaimed Property by phone at **1-888-258-2253** or start your search online at **FLTreasureHunt.gov**.

DIVISION OF WORKERS' COMPENSATION

The Division of Workers' Compensation is responsible for ensuring individuals interested or involved in the workers' compensation system have the tools and resources they need to participate. The Division assists injured workers, employers and health care providers in following the workers' compensation rules and laws. The Division also enforces the workers' compensation coverage requirements. To verify that a contractor has workers' compensation insurance call **(850) 413-1609** or visit the website at **MyFloridaCFO.com/Division/WC**.

EXTERNAL RESOURCES

ELDER CARE SERVICES, INC.

Elder Care Services provides information and resources on aging issues, services and programs affecting seniors in the Big Bend area. Services include: In-home Care Management, Elder Day Stay, Meals on Wheels and the Senior Volunteer Program. For additional information call **(850) 921-5554** or visit the website at **ElderCareBigBend.org**.

FLORIDA DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

To verify a contractor's license and their contractor number, you can call **(850) 487-1395** or visit **MyFloridaLicense.com/DBPR/**.

FLORIDA DEPARTMENT OF ELDER AFFAIRS
The Department of Elder Affairs provides direct services to Florida residents ages 60 and older. The Department administers a wide range of programs such as: the Long-Term Ombudsman Program, Communities for a Lifetime, SHINE (Serving Health Insurance Needs of Elderly) and CARES (Comprehensive Assessment and Review for Long-Term Care Services). For additional information about programs and services call the toll-free Elder Helpline at **1-800-96-ELDER (1-800-963-5337)** or visit **ElderAffairs.org**.

FLORIDA OFFICE OF THE ATTORNEY GENERAL, SENIORS VS. CRIME
Seniors vs. Crime is a group of volunteer senior advocates who are actively involved in protecting their communities and fellow seniors from becoming victims of fraud. Volunteers investigate and attempt to resolve complaints they receive from seniors in the local community. Services are free of charge and all recoveries are returned to the victim. For additional information visit **SeniorsVsCrime.com**.

NATIONAL AND FLORIDA DO NOT CALL REGISTRY
The National and Florida Do Not Call Registries allow you to remove your name from telemarketing call lists. For the National Do Not Call Registry, call **1-888-382-1222** or visit **DoNotCall.gov**. For the Florida Do Not Call Registry, call **1-800-435-7352**, outside Florida call **850-410-3800** or visit **FDACS.gov/Consumer-Resources/Florida-Do-Not-Call.**

ANNUALCREDITREPORT.COM
To obtain a free copy of your credit report, visit **AnnualCreditReport.com** or call **1-877-322-8228**.

CREDIT BUREAU CONTACT INFORMATION
To dispute a line of credit opened in your name or for additional information regarding your credit history, contact the credit bureaus listed below.

EQUIFAX
Equifax.com
P.O. Box 740256
Atlanta, GA 30374
1-800-525-6285

EXPERIAN
Experian.com
P.O. Box 4500
Allen, TX 75013
1-888-397-3742

TRANSUNION
TransUnion.com
P.O. Box 2000
Chester, PA 19022
1-800-680-7289

ADDITIONAL RESOURCES

Visit the websites below for additional information on a wide range of financial topics.

MyFloridaCFO.com

MyFloridaCFO.com/Division/Consumers

MyFloridaCFO.com/Division/Consumers/ConsumerProtections/AssignmentOfBenefits

MyFloridaCFO.com/SAFE

MyFloridaCFO.com/YMM

FLOFR.gov

FBI.gov/Scams-and-Safety

FBI.gov/Scams-and-Safety/Common-Scams-and-Crimes

FDACS.gov/

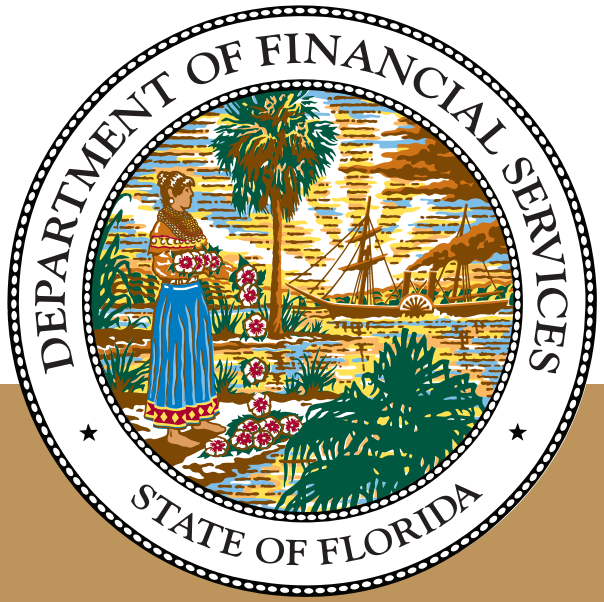
FTC.gov

HUD.gov/Program_Offices/Housing/SFH/HECM/HECMhome

BE SCAM SMART

OPERATION S.A.F.E.

STOP ADULT FINANCIAL EXPLOITATION



March 2023