Savvy Consumers Can Stop Fraud

A Guide for Seniors

Office of the Attorney General
Ashley Moody

Table of Contents

Letter from Attorney General Ashley Moody 4

Safeguarding Finances 5

Identity Theft 7

Reverse Mortgages and Foreclosure Rescue Firms 14

Contractors and Home Repair 16

Scams that Target Seniors 19

- *Imposter Scams* 19
- *Telemarketing Scams* 20
- *Discount Prescription Programs* 20
- *Tech Support Scams* 20
- *Medical Alert and Security System Scams* 21

Travel Scams 22

Charity Scams 23

Seniors vs. Crime 24

- *Seniors vs. Crime Regions Map* 26

Dear Fellow Floridian:

Florida is the third most populated state in the union with over 21 million residents calling Florida home. In 2018, a record breaking 126.1 million people visited the Sunshine State, setting a tourism record for the eighth consecutive year. Unfortunately, Florida is also number one in cases of fraud. With so many people living and visiting our great state, many of them senior citizens, it is imperative that we, as a state, do better in educating, preventing, and attacking fraudsters and scam artists who prey on the vulnerable.

As your Attorney General, I am tasked with enforcing our state laws and making sure we go after those who defraud and exploit our seniors. Within the first two months of taking office, I put together a team of experts within the Attorney General's Office and agents statewide to focus on protecting our senior citizens from fraud, scams, and exploitation. I am committed to providing our seniors with the information and tips they need to help them avoid becoming victims.

My office, along with its federal, state, and local agency partners, all work hard to combat fraud, but you have a role in this effort as well. You can help stop the con-artists before they strike by learning to recognize scams for what they are. To assist you, my office has created this resource guide. We hope it helps you avoid potential scams. We also hope it generates discussion among you and your family, friends, co-workers, and neighbors about ways to guard against consumer fraud. Helping spread the word and educate those around you will help us eliminate fraud and could help prevent someone you know from becoming a victim. This guide offers information on identity theft, imposter scams, debt collection, fraudulent contractors and much more.

I hope you will find this guide a helpful resource. I encourage you to contact my office at 1-866-9-NO-SCAM (1-866-966-7226) or online at **www.MyFloridaLegal.com** if you have any questions about this guide or if you have been the victim of unfair or deceptive business practices.

We are here to serve you.

All my best,

Ashley Moody

Ashley Moody

Safeguarding Finances

Seniors are the primary target of investment and financial fraud.

Common Types Of Investment Fraud

Ponzi schemes: A Ponzi scheme is a scheme in which investors are usually promised an unrealistic rate of return in exchange for an investment. The funds are not invested as represented and initial investors are paid interest and principal from new investors and not from investment activity. The scheme collapses when new investments no longer can sustain the interest and principal payments. At that point there is little left for investors to recover.

"Free lunch" seminars: Investors are baited into attending seminars with offers of free lunch, dinner or prizes, during which they are offered investments that have "guaranteed" returns and "little or no risk at all." Often the products offered at such seminars are investments that produce the greatest amount of profit or commission for the broker and his firm, but provide little or nothing to the investor.

Unlicensed brokers: Unscrupulous individuals sell unlicensed securities promising huge investment returns. Investors typically lose the money they have invested.

Tips To Avoid Financial And Investment Fraud:

Consider the following tips prior to investing:

- Use Financial Industry Regulatory Authority's (FINRA) BrokerCheck at www.finra.org/brokercheck or call the FINRA Hotline at (***800***) ***289-9999*** to see if a broker is registered and whether they have a disciplinary record with the organization.
- Ask for references and check with the Better Business Bureau (www.bbb.org) and the Florida Office of Financial Regulation (www.flofr.com) for complaints against the broker or the firm.
- Ask any broker whether the broker and his or her firm are registered with FINRA, the Securities and Exchange Commission (SEC) and the state Office of Financial Regulation.
- If seeking the assistance of an attorney, check with the Florida Bar to ensure the attorney is in good standing with no disciplinary record. The Florida Bar's website is www.FloridaBar.org.
- Consider seeking consultations from several brokers or attorneys. Many offer free consultations that will help clients determine if they are a good fit.
- Contact the Public Investors Arbitration Bar Association (www.piaba.org) a national organization of attorneys who represent investors. They can assist consumers in finding an experienced attorney in their community.
- When choosing particular investments, ask whether the investment is registered with the SEC.
- Avoid investments that promise huge profits with little or no risk. No investment can guarantee profits and legitimate brokers will inform consumers of risks involved.
- Ask the broker or advisor how he or she is compensated. Is he or she paid on commission based on investment choices of clients or does he or she charge a standard hourly rate?

Consider the following tips to keep funds safe:

- Check account statements regularly to ensure there are no fraudulent charges or withdrawals.

- Keep checkbooks and debit and credit cards in a safe place. Never leave them in view around the house, particularly if there are non-family members in the home.
- Consider a banking institution that offers custodial accounts, wherein the bank collects the individual's income and pays their bills.

Financial Abuse

According to the Securities Industry and Financial Markets Association (SIFMA), U.S. seniors lose as much as $2.9 billion per year to financial exploitation. Unscrupulous individuals target senior citizens with diminished physical or mental capacity. It is important to know what to look for to protect a vulnerable adult.

Indicators of potential financial abuse can include the following:

- Suspicious or sudden change to a will or powers of attorney;
- Financial activity or charges a vulnerable adult could not or would not have made themselves;
- Unpaid bills indicating that a vulnerable adult is in need of assistance;
- Valuable belongings or prized family heirlooms missing; and
- Suspicious signatures on checks or legal documents.

Identity Theft

Consumers become identity theft victims every day, and recovering from it can be a lengthy and involved process.

What Constitutes Identity Theft?

As defined by federal law, identity theft occurs when someone uses or attempts to use the private personal information of another person to commit fraud, typically for economic gain. A wide range of information constitutes private personal information which can be used to commit identity theft. This can include a person's name, address, date of birth, Social Security number, driver's license number, credit card and bank account numbers, phone numbers and even biometric data like fingerprints and iris scans.

Signs Identity Theft Has Occurred

Red flags that indicate a consumer's identity has been stolen include:

- Being denied access to credit;
- Finding suspicious charges on bank or credit card statements;
- Receiving a notice that private personal information has been compromised in a data breach;
- Becoming aware that someone has fraudulently forwarded the consumer's mail or that the consumer has stopped receiving credit card bills;
- Finding errors in a credit report, such as a loan or account not opened by the consumer;
- Encountering issues with medical insurance, such as a denial of coverage or bills for a treatment he or she never received;
- Being denied state or federal benefits because the consumer is listed as already having received them;
- Having his or her tax return rejected by the IRS because the refund has already been claimed; or
- Receiving calls from a debt collector regarding a debt not owed.

Steps To Take When Identity Theft Has Occurred

The following steps should be taken immediately after learning of an incident of identity theft:

STEP 1: Contact the police. File a report with law enforcement. Under Florida Statute Section 817.568(18), consumers may file a report in the location where the theft occurred or in the city or county in which they reside. When filing, consumers should provide as much documentation as possible, including copies of debt collection letters, statements showing fraudulent charges, credit reports and any other evidence they may have. Request a copy of the police report; creditors and credit reporting agencies may request to see it before removing the debts created by the identity theft from their records.

STEP 2: Report the incident to the fraud department of the three major credit bureaus. Consumers should contact the credit bureaus to place fraud alerts on their credit report. Consumers should also order copies of their credit reports to determine whether there are additional fraudulent accounts listed in their names. Contact information for the three major credit bureaus is as follows:

Equifax
To report fraud: ***1-800-525-6285***
To order a credit report: ***1-800-685-1111***
www.equifax.com

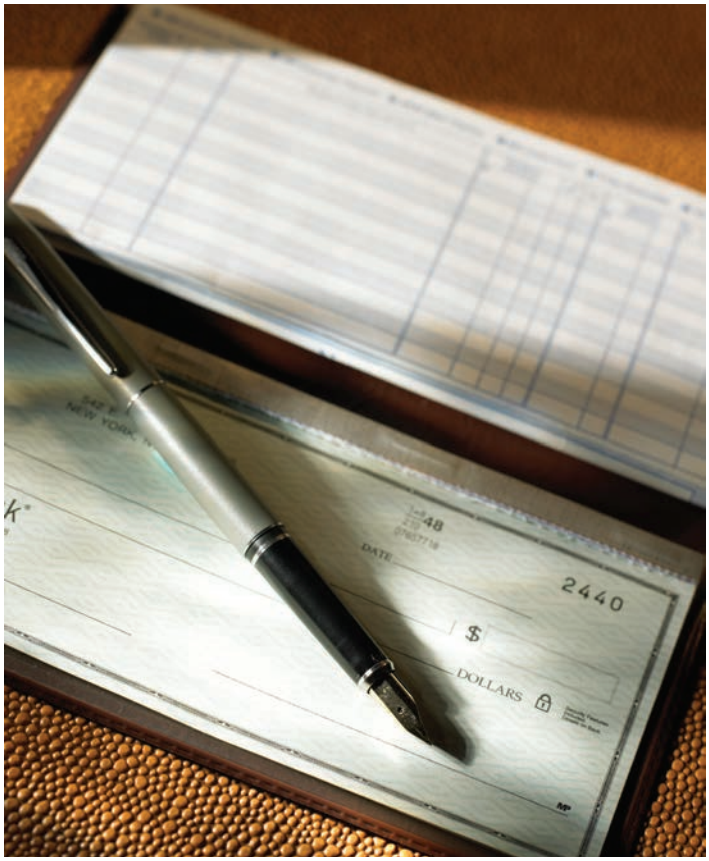
Experian
To report fraud: ***1-888-397-3742***
To order a credit report: ***1-888-397-3742***
www.experian.com

TransUnion
To report fraud: ***1-800-680-7289***
To order a credit report: ***1-800-888-4213***
www.transunion.com

STEP 3: Contact the fraud department of each creditor. Consumers should gather the contact information for each of their credit accounts (credit cards, retail credit accounts, utilities, cable and Internet providers, etc.) and call the fraud department for each. Report the incident to each creditor, even if the account at that institution has not been affected. Consumers should close accounts that they believe have been compromised. Request the creditors place an alert on any accounts that remain open and follow up in writing.

STEP 4: Report identity theft to the Federal Trade Commission. The FTC provides a standardized Identity Theft Affidavit and action plan for victims of identity theft at **www.IdentityTheft.gov**. It is important to complete this form as some creditors will not begin an investigation or remove fraudulent activity from their records until they receive it. Check with each creditor to determine if it accepts this form; if not, request a copy the creditor's fraud dispute form and complete it.

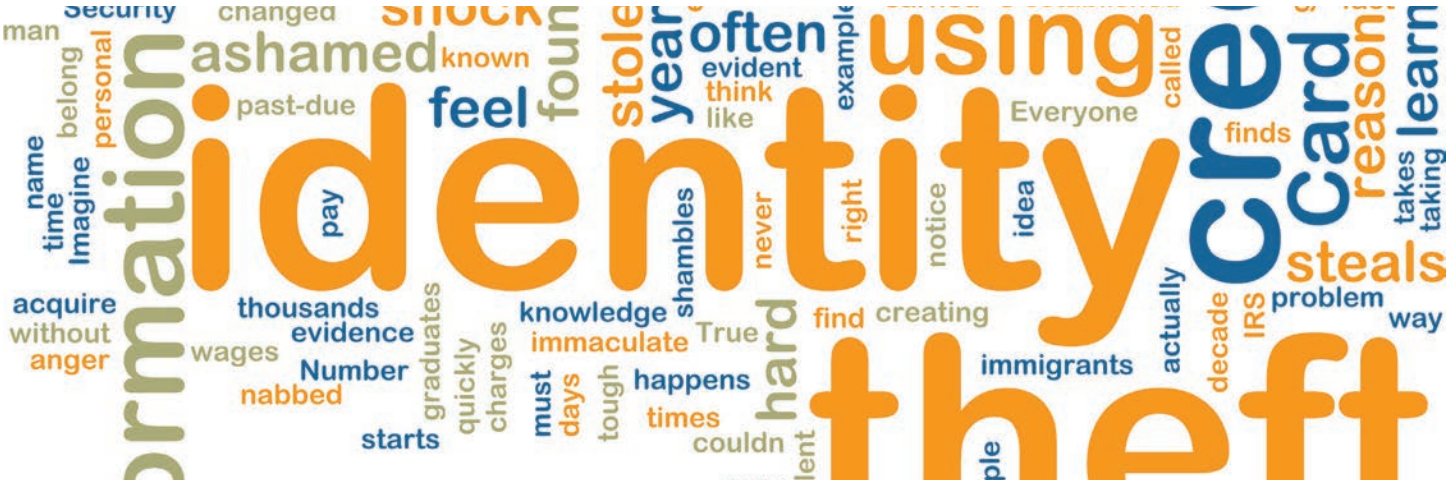
STEP 5: Contact banks or financial institutions. If consumers suspect their financial accounts have been compromised, they should close their checking and savings accounts. They should also ask that their banks issue not only new debit card numbers, but also new account numbers. Put stop payments on any suspicious outstanding checks. Consumers whose checks have been stolen should contact the major check verification companies and request they notify retailers not to accept their checks. These services allow businesses to determine whether a check is valid and can be reached at:



TeleCheck
1-800-710-9898

ChexSystems
1-800-428-9623

Consumers should also call Certegy Check Services at ***1-800-437-5120*** to determine whether any bad checks have been passed in their name.



Other Action To Take Following Identity Theft

Consumers should take the following actions, as applicable, to repair and protect their credit:

- **File a complaint with state and federal authorities.** Consumers should file a complaint with the Florida Attorney General's Office using the toll-free fraud hotline at ***1-866-9-NO-SCAM*** or by visiting online at www.MyFloridaLegal.com. Consumers should also file a complaint with the FTC's Identity Theft Clearinghouse. Complaint information filed with the FTC is entered into a central database, the Consumer Sentinel. Consumers may call the FTC's toll-free hotline at ***1-877-IDTHEFT*** or complete an online complaint form at www.FTCcomplaintassistant.gov.

- **Report a lost or stolen Social Security card to the Social Security Administration.** Consumers may determine whether someone is using their Social Security number for work by creating an account and reviewing their Social Security work history at www.socialsecurity.gov/myaccount. Consumers may apply online for a free Social Security replacement card at www.ssa.gov/ssnumber.

- **Report passport fraud to the U.S. Department of State.** Consumers whose passports have been stolen should contact the Department of State at ***1-877-487-2778***.

- **Place a flag on Florida driver license.** Consumers with a Florida driver license should flag it with the Fraud Section of the Department of Highway Safety and Motor Vehicles. To place a flag, consumers may email fraud@flhsmv.gov or call ***850-617-2405***.

- **Check for fraudulent Florida criminal records.** In some instances, an identity theft victim may be faced with a criminal record for a crime he or she did not commit. The Florida Department of Law Enforcement (FDLE) can provide a Compromised Identity Review to determine if any arrest records have been falsely associated with the victim as a result of identity theft. Those who believe their identities have been compromised should initiate a review by contacting FDLE at: ***850-410-7000***

- **Remove personal identifiers from Florida court records.** Any person has the right to request the Clerk or County Recorder redact or remove his or her Social Security number, bank account number, credit or debit card number from an image or copy of an Official Record that has been placed on the Clerk's or County Recorder's publicly available website or in a court file. Consumers may contact the local County Clerk's Office to initiate a request. Check the State of Florida Clerk Directory for each county's contact information at www.flclerks.com.

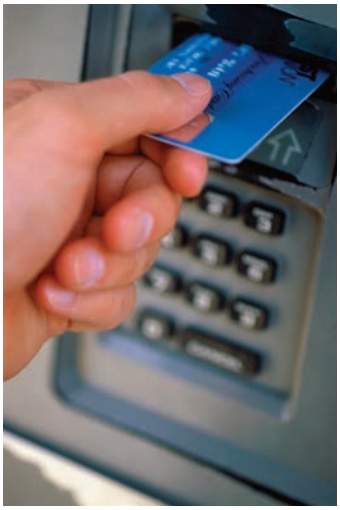
- **Report mail theft to the U.S. Postal Inspection Service.** The U.S. Postal Inspection Service will investigate if a consumer's mail has been stolen by an identity thief. Incidents should be reported to the U.S. Postal Inspection Service. Consumers may file a complaint online at www.postalinspectors.uspis.gov.

Limits On Financial Loss Resulting From Identity Theft

Both federal and state laws limit an identity theft victim's financial losses. Under state law, no identity theft victim may be held liable for any unauthorized charges made on a credit card that is issued on an unsolicited basis. Under federal law, the amount an identity theft victim must pay for unauthorized credit card charges is limited to $50. If a victim reports the identity theft prior to unauthorized charges being made, the victim is not responsible for any charges. Under federal law, the amount an identity theft victim must pay for unauthorized charges made on an ATM or debit card varies based upon how quickly the loss is reported.

- If a victim reports the loss or theft of an ATM or debit card prior to unauthorized charges being made, the victim is not liable for any losses.
- If a victim reports the loss or theft within two business days of learning of it, the maximum loss is $50.
- If a victim reports the loss or theft more than two business days after learning of it but fewer than 60 calendar days after receiving a bank statement, the victim's maximum loss is $500.
- If a victim reports the loss or theft more than 60 calendar days after receiving a bank statement, the maximum loss is potentially unlimited.

If an unauthorized charge is made to a victim's bank account using the victim's debit card number but not the physical debit card, the victim is not responsible for the unauthorized charges as long as it is reported within 60 calendar days of receiving a bank statement on which the charges first appear.



Individual financial and credit institutions may waive a victim's responsibility for unauthorized charges as a benefit to their members and cardholders. Consumers should check the terms and conditions of their financial accounts to determine whether they will be held liable for any unauthorized charges.

Protect Personal Information

Keeping personal information safe, both online and off, is a key facet of guarding against identity theft. Offline, consumers should take care to do the following:

- Read account statements each month to ensure there are no fraudulent charges.
- Do not respond to emails, text messages or phone calls that ask for personal information. If a consumer believes the request could be a legitimate communication from a company with which he or she does business, they should contact the company at the phone number listed on their bill or account statement and inquire whether the communication is legitimate.
- Lock documents and records in a safe place at home or in a safe deposit box at the bank. Keep personal information, credit and debit cards and checks secure from guests or workers who come into the home.
- Limit what they carry. Bring only the identification, credit and debit cards necessary. Consumers should not keep their Social Security card in their wallet.
- Consider photocopying wallet contents and keep the copies in a safe or safety deposit box. This way if a consumer's wallet is stolen, he or she can report exactly what information the thieves obtained and know which companies to contact about canceling cards and closing accounts.
- Destroy the labels on prescription bottles before throwing them out.
- Before sharing personal information, such as

a Social Security number, at the workplace, a business, a school or a doctor's office, consumers should ask why the business needs it, how it will be secured and the consequences should they choose not to provide the information.

- Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards and similar documents when they are no longer necessary.
- Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in the mailbox. Consumers should request a vacation hold on their mail and newspapers if they will not be home for several days.
- Consider opting out of prescreened and preapproved credit offers that are received by mail. Consumers may opt out permanently or for a period of 5 years by visiting **www.optoutprescreen.com**. Consumers may opt back in at any time using the same website.
- Check credit reports at least once a year. Consumers have the right to a free credit report each year from each of the three major credit reporting agencies. To order a credit report, go to **www.annualcreditreport.com**.

When online, consumers should take care to do the following:

- When ordering something online, look to ensure that the browser has a secure connection. In the address bar, a padlock should appear if the browser is secure.
- Use strong passwords that include letters, numbers and special characters and cannot be easily guessed. Additionally, do not use a single password across multiple websites.
- Some credit card providers offer one-time card numbers to be used for online transactions to further protect consumer financial information. Consumers should contact their account holder to see if they have access such a service.
- Never include personal or financial information in an email.
- Know that a financial institution will never email account holders a link for them to "confirm" their account number or "verify" their log-in details.
- Choose strong secret questions. Secret questions are often used to reset accounts if the user cannot remember his or her password. Do not use a secret question that can be easily guessed.
- Ignore pop-up windows that say the computer has a virus or is infected with malware.
- Do not use public wireless networks, such as those available in hotels or coffee shops, to perform financial transactions.
- Install anti-virus and anti-spyware software on computers.
- Ensure a computer's operating system and web browser are up to date. Change settings so these updates are applied automatically.

Credit Report Basics

A credit report can be a crucial tool that allows consumers to know where they stand financially and can also indicate whether their identity has been stolen. A credit report includes information on where the consumer lives, how he or she pays their bills and whether they have been sued or have filed for bankruptcy. A credit report and credit score offer an indication of whether a consumer is a good risk for lenders.

Under the Fair and Accurate Credit Transactions Act, an amendment to the federal Fair Credit Reporting Act passed in 2003, consumers are able to receive one free credit report per year from each of the nationwide credit reporting companies — Equifax, Experian and TransUnion. The free report can be requested and viewed online through the government-authorized website **www.annualcreditreport.com**. While consumers may receive a credit report for free, reporting agencies often charge a fee to provide an individual with his or her specific credit score.

Reverse Mortgages and Foreclosure Rescue

While reverse mortgages may sound like a great deal, they are not suitable for everyone.

How Reverse Mortgages Work

A reverse mortgage converts the home's equity into cash payments to the homeowner. The money received is generally tax-free and the loan does not have to be paid back as long as the homeowner lives in the home. The loan will become due when the homeowner dies, fails to pay taxes or insurance on the home, lets the home fall into disrepair, sells the home, or no longer uses the home as his or her primary residence. This means should the homeowner's heirs wish to retain the home, they will need to pay the lesser of the laon balance including interest and fees or 95% of the fair market value of the home.

Consider the following before deciding to take out a reverse mortgage on your home:

- There are additional fees and costs associated with acquiring a reverse mortgage. There are generally closing costs and servicing fees. Some lenders may also charge mortgage insurance premiums.
- Interest will accrue each month, increasing the amount owed over time.
- Interest is not tax deductible on income tax returns until the loan is paid off.
- Know that the homeowner must pay property taxes, carry homeowner's insurance and maintain the condition of the home, otherwise the loan may become due.
- Compare fees and costs across lenders to determine which will offer the best deal.
- Never let a lender pressure or rush through the process. Understand the features and total cost of a reverse mortgage before signing anything.

Foreclosure Scams

Mortgage "rescue" firms claim to be able to assist with obtaining a modified mortgage so homeowners can avoid foreclosure. Unscrupulous "rescue" firms charge exorbitant fees while promising relief that never comes. While some mortgage brokers offer legitimate services, consumers should first contact the bank that holds their mortgage. The lender's loss mitigation specialist can often, at no charge, present available options. There are also HUD-certified housing counselors nationwide who may be able to offer advice and assistance. Consumers can find a HUD counselor in their area at **www.hud.gov** or can call their toll-free hotline at 1-***888-995-HOPE***.

Should consumers seek the advice of an attorney, they should verify the attorney is in good standing with no disciplinary record with The Florida Bar at **www.FloridaBar.org**.

Consumers can verify a mortgage broker's license on the Office of Financial Regulation's website at **www.flofr.com**. Under Florida law, a "rescue" firm or mortgage broker may never charge consumers up front for their services. Brokers may only charge consumers after receipt and acceptance of a written offer for a loan or refinance contract. Consumers who have complaints about their mortgage servicer or broker should file a complaint with our Office online at **www.MyFloridaLegal.com** or by calling ***1-866-9-NO-SCAM*** toll-free in Florida.

Contractors and Home Repair

Unscrupulous individuals seek to take advantage of seniors by convincing them that their homes are in need of urgent repair.

Finding A Contractor

Qualified contractors are in high demand, making conditions ideal for scam artists. Consider the following tips when hiring a contractor:

- Be wary of anyone who approaches unsolicited or says they can perform home repairs at a discount with leftover supplies from another job.
- Following any home damage, have the insurance company evaluate the damage before arranging repairs to ensure that the work will be covered under the policy.
- Get at least three written, itemized estimates or bids on repairs.
- Verify that the contractor has a license from the Department of Business & Professional Regulation and the county construction licensing board, if applicable. A licensed contractor can be looked up and verified on the DPBR website at **www.MyFloridaLicense.com**.
- Research the company and its reputation – ask for references. In addition to DPBR, consumers should check with the Better Business Bureau at **www.bbb.org** to see if there are complaints against the company.
- Check for proof of insurance and verify with the insurer that the company's policy is current.
- Check to see if the contractor is bonded and verify with the bonding agency.
- Never pay the full amount of a repair up front and hesitate before providing large deposits. Florida law requires a contractor to apply for a permit within 30 days and start work within 90 days if he collects more than 10 percent of the contract up front.

- Read the entire contract, including the fine print, before signing and ensure that the contract includes the required "buyer's right to cancel" (within 3 days) language.
- Homeowners may unknowingly have liens placed against their properties by suppliers or subcontractors who have not been paid by the contractor. If the contractor fails to pay them, the liens will remain on the title. Insist on releases of any liens that could be placed on the property from all subcontractors prior to making final payments.
- Do not sign a certificate of completion or make final payment until completely satisfied with the work.

Assignment of Benefits

An Assignment of Benefits (AOB) is a document that allows insurance policyholders to sign over their insurance rights or benefits to a third party. This

allows the third party to file an insurance claim, make repair decisions and collect on benefits without the policyholder's involvement. While Assignments of Benefits can offer convenience to policyholders attempting to navigate the insurance claims process, unscrupulous individuals and companies may seek to take advantage of the power an AOB provides them. Consider the following tips before signing over benefits:

- Know that you are not required to sign an AOB in order to have repairs made or to process an insurance claim.
- Be wary of any company that pressures you to sign or insists upon the use of an AOB in order to do repairs.
- Some unscrupulous contractors may attempt to hide an Assignment of Benefits within a lengthy repair contract. Read the entire contract carefully to ensure you are not signing over your benefits without your full knowledge and consent.
- Know that you may be responsible for any additional costs not covered by insurance, and that a contractor may place a lien on your home if you fail to pay.
- Know that AOBs are legally binding and offer no right to cancel after they have been executed.
- Know that an AOB contains language that, once executed, would prevent you from communicating with your insurance company about the claim.
- Do not sign an AOB if there are blank spaces in the document.

Water Testing and Treatment

Dishonest companies offer pricey tests and devices to make water "safe." Avoid falling victim by following these tips:

- If someone claims to be with the city, county or utility provider needing to inspect the water line or well, ask for proof of identification.
- Check with local media for any water safety alerts. If in doubt the water's safety, contact the local health department or utility. Local water utilities are required to test water quality on a regular basis.

Air Conditioning Repair

Some untrustworthy air conditioning repair companies offer duct cleaning or inspections at a low cost then claim to find something that needs urgent repair at an exorbitant price. Consider the following tips before hiring an A/C repair company:

- Be wary of free or low-cost A/C or duct inspection offers.
- Seek out a second opinion, particularly if a company has approached you unsolicited to perform a repair or clean your ducts.
- Check to see whether the current air conditioning unit is still covered by a manufacturer's warranty before agreeing to any repairs.
- Research the company and its reputation. Check with the Better Business Bureau at **www.bbb.org** to see if there are complaints against the company.
- Check for proof of insurance and verify with the insurer that the company's policy is current.

Scams that Target Seniors

While the scams below can affect consumers of all ages, the perpetrators often specifically target seniors.

Imposter Scams

In these schemes, scam artists pose as family members, trusted friendws, law enforcement officers or government agency representatives and request or demand money via prepaid debit cards, gift cards or wire transfers immediately to help a loved one in need, avoid penalties or to claim a prize.

The Grandparents Scam: One version of this scam involves imposters posing as law enforcement officers calling grandparents and claiming that a grandchild is in jail. The imposters then demand immediate payment to bail the grandchild out of jail. In another version of the scam, a person claiming to be a grandchild will call saying that he or she has been injuared or detained in another country and needs money to get home. Avoid acting immediately and verify the grandchild's whereabouts with an other family member.

Romance Scams: Imposters pose as individuals on dating sites, social media sites, or even in person in an attempt to forge an emotional connect with potential victims. Once the imposter has formed a connection with an individual, they claim they need money urgently to cover an emergency, deal with a family situation, take advantage of a business opportunity, recover from theft or a stolen identity, or to travel to meet them. Prior to sending money, signing over property or providing gifts to a new friend, consult a financial advisor, attorney or a trusted friend or family member.

The Jury Duty Scam: This scam typically involves imposters posing as law enforcement officers and calling or emailing a victim claiming that the victim has missed jury duty. The imposters claim the victim must pay a fine immediately or face arrest. Be aware that a court official will never ask a consumer to wire money or ask for personal or confidential information over the phone or via email.

Arrest Warrant Scam: In this scam, imposters pose as law enforcement officers and call or email a victim claiming that they have a warrant out for the victim's arrest or that the victim is otherwise being pursued by law enforcement. The imposters will claim the victim must pay them immediately or be arrested. Know that a law enforcement or court official will never ask a consumer to wire money or ask for personal or confidential information over the phone or via email.

Utility Scams: This scam involves imposters claiming to be from one of the utilities in Florida and threatening to turn off the power, gas or water unless a payment is made. Consumers receiving these calls should hang up and contact their utility provider using the phone number that appears on their bill to determine the account's status. No legitimate utility would phone and make such threats. Report any fraudulent utilities calls to the utility provider.

Sweepstakes/Lottery Scams: A typical version of this scam includes imposters claiming to be with the Governor's Office, Attorney General's Office or a private law firm calling or emailing a potential victim saying the victim has won the Publisher's Clearinghouse sweepstakes, another sweepstakes or a foreign lottery. Callers often identify themselves as U.S. Customs officials, lawyers for a government agency or lottery officials. Victims are told they need to pay customs duties and taxes before the winnings can be sent to them. Legitimate sweepstakes do not require consumers to pay anything to receive the prize he or she has purportedly won. Consumers told that they must pre-pay taxes are likely being scammed.

With legitimate sweepstakes, taxes are either withheld from the cash award or, more commonly, are reported by the company to the IRS and the consumer must declare the prize as part of his or her annual tax return. Consumers should also know that participating in a foreign lottery is against federal law, so any claim they have won a foreign lottery is a scam.
IRS Scam: In this scam, imposters pose as IRS agents and call or email potential victims claiming that they owe the IRS taxes. The scammers claim that unless they are paid immediately, the consumer will be arrested. The imposters demand to be paid via money wire or a prepaid debit card. Know that the IRS will never make first contact via email or over the phone. They will always make first contact by mail. Should a consumer receive a letter claiming to be from the IRS, he or she should confirm the number listed is a legitimate contact number for the IRS. The IRS also will never demand that a consumer wire money or provide a prepaid debit card for payment.

Telemarketing Scams

The hallmark of this scam is a scam artist calling a potential victim and selling products using high-pressure sales tactics. The scammer urges the victim to act immediately or risk losing out on a great deal or a "free" prize offer. Consumers should hang up if they feel pressured or the sales person refuses to provide more information. They should not provide personal financial information unless they are certain the business is legitimate. Consumers should also register their landline and mobile phone numbers on the national Do Not Call list at **www.DoNotCall.gov** and the Florida Do Not Call list at **www.fldnc.com**.

Discount Prescription Programs

While some medical discount programs offer legitimate savings to the consumer, some engage in deceptive practices or outright fraud. Some discount programs require exorbitant monthly or annual fees before a consumer can access any savings. Some discount cards are only valid with name-brand medications, so the consumer may see more savings by purchasing generic brands. Some programs use tactics that lead consumers to believe that they are purchasing insurance coverage. Consumers should not sign up for a program in which the benefits are not clearly defined.

To compare the prices of the 300 most commonly prescribed medications, use **www.MyFloridaRx.com**. MyFloridaRx was created by the Attorney General in conjunction with the Florida Agency for Health Care Administration to assist citizens in finding the cheapest prescriptions in their area.

Tech Support Scams

There are several ruses that scammers use to perpetrate a tech support scam. In one common ruse, the scam artist will call a potential victim claiming to be a representative from Microsoft or another major computer software or tech company. The caller will say that the company has detected a virus or malware on the victim's computer. The scammer will then ask for remote access to the computer to further "diagnose" and "fix" the computer for a fee.

In another common ruse, the scam artist will use pop-up advertisements claiming that the consumer's computer is infected with a virus and explain that a number must be called to correct the problem. Once called, the scammer will ask to remotely access the computer. When the scam artists remotely log in to the

computer, they often complete a "diagnostic," showing consumers several different screens and claiming that the screens show problems with the consumer's computer that require immediate action. They then offer to fix the computer for a fee or insist the victim needs to purchase particular security software. At best, this software is likely available for free or much cheaper elsewhere; at worst, this software may be malware designed to access confidential information.

Before accepting any offer of computer technical support, consider the following:

- Be wary of anyone calling claiming to be from a legitimate company to warn of a computer virus or infection.
- Do not allow anyone who makes an unsolicited tech support call to have remote access to computers.
- Know that online search results may not be the most reliable way to find technical support or get a software company's contact information. Scammers may pay to boost their search result rankings to appear above the listings of legitimate services.
- When in need of technical support, seek out a trusted repair person or seek advice at an established electronics or computer retailer.
- Know that scammers use online ads that look like computer warnings to convince victims to call them or download their software.
- Do not click on an Internet pop-up that claims that the computer is infected with a virus or malware. Should the pop-up list a phone number to call, do not call that number. Instead, seek a legitimate repair company to address any concerns.
- Do not give out sensitive information, such as credit card numbers and passwords, over the phone or via email.

Medical Alert and Security System Scams

With this scam, a technician or salesperson claiming to be a representative of a consumer's current security system provider appears at the consumer's door. The representative tells the consumer that their system is out of date, in need of upgrades or their current provider is going out of business. Once the consumer signs up, the consumer discovers that he or she is being billed for two security systems, the consumer's existing, legitimate security system provider and the "new" or "updated" system. Before signing any security system contract, consider the following:

- Ask for photo identification and a business card from anyone who appears at the front door claiming to be a representative from the current security system company.
- Call the current security company at the number listed on the bill to confirm all claims.
- Ask for references and quotes from competing companies before signing any contracts and check with this Office and the Better Business Bureau for complaints.
- Do not feel pressured into agreeing to new equipment or signing a contract.
- Request literature be left behind and study it before taking action.
- Know what is included in the price and whether the quote given includes all equipment, fees and charges before signing any contracts.
- Know what the cancellation policy and any associated charges are.
- Report any suspicious activity to the fraud hotline by calling ***1-866-9-NO-SCAM (1-866-966-7226)*** or by visiting **MyFloridaLegal.com**.

Travel Scams

Prevalent travel scams include discount travel clubs, vacation prizes and timeshare-related scams.

Discount Travel Clubs

With this scam, consumers are told once they join a travel club or a buy a discount travel card, they will receive a free vacation. These discounts often cost several hundred dollars, yet some consumers who sign up never receive their free vacations or they are told that the dates they have chosen are unavailable. Other consumers pay for the travel club only to have the company close down. Some consumers who are able to use the travel discounts find later that they paid the same or more than consumers who are not travel club members.

Vacation Prize Packages

This scam typically involves consumers receiving postcards telling them that they have won a free vacation. Generally, the "winners" must call a number to claim their prize. When the consumer calls, the business offers to send information about the vacation package only after the consumer provides his or her credit card so that a small "service charge" can be assessed or "taxes" can be withheld. Once the consumer has been charged, the consumer's promised vacation never materializes or the dates chosen are blocked out.

Timeshare Scams

In this scam, consumers are invited to a timeshare sales presentation after which they are told they will receive a particular "free" gift. Instead, after the presentation, consumers are subjected to high-pressure timeshare sales pitches. Consumers who purchase timeshares under this pressure and wish later to cancel are often unable to do so, even within the stated cancellation period. In the timeshare resale version of this scam, consumers who currently own timeshares and are interested in selling are contacted by the scammer and told that there is a buyer ready, willing and able to purchase the consumer's timeshare at an inflated price. The timeshare owner is asked to pay up-front fees for "closing costs," "deed searches and transfers" or "taxes." When the sale never materializes, the timeshare owner is unable to get a refund. Consumers should know that it is illegal for a timeshare resale company to require an up-front fee over $75.00 without complying with contractual requirements under Florida Statute Section 721.205 or to misrepresent the existence of a ready, willing and able buyer. Also, consumers should always be wary of offers that sound too good. Report scams to the Office of the Attorney General at ***1-866-9-NO-SCAM*** or online at **www.MyFloridaLegal.com**.

Charity Scams

Unscrupulous "charity" operators look to cash in on the support offered to the various charitable causes by people who care.

Signs Of A Charity Scam

Red flags consumers should look for indicating that a charity is not legitimate include:

- The charity or solicitor refuses to provide detailed information about the charity's mission, fundraising costs and use of donations;
- The solicitor uses high-pressure or guilt tactics to get donations;
- The solicitor requests donations be made in cash, via prepaid debit card or be wired to a particular account;
- The charity has sent an unsolicited email encouraging recipients to enter credit card or bank account information to donate;
- The solicitor offers to send a courier to collect the donation immediately;
- The solicitor asks for the check to be made to a particular person rather than the organization; or
- The charity's name closely resembles that of a large, well-known and highly regarded charity.

Check A Charity's Legitimacy

To determine whether a charity soliciting funds is legitimate, first check to see if it is a registered charity with the state Department of Agriculture and Consumers Services (DACS). Consumers may check the DACS Gift Giver's Guide to determine whether a charity is registered and what percentage of their revenue goes to providing actual services at **www.800helpfla.com**.

Consumers should also check with the Internal Revenue Service to see if the tax-exempt organization filed an annual return. The IRS requires revocation of a charity's tax-exempt status if it fails to file a return for three consecutive years. To learn more, go to **IRS.gov** and search the Charities and Non-Profits topics.

Finally, consumers may also contact the Department of Agriculture and Consumer Services at ***1-800-HELP-FLA***, this Office at ***1-866-9-NO-SCAM***, or the Better Business Bureau's Wise Giving Alliance at **www.give.org** or Charity Navigator at www.**CharityNavigator.org** to determine whether the charity has complaints against them.

Seniors vs. Crime

The Seniors vs. Crime project gives seniors a safe, non-judgmental place to report consumer fraud and scams.

An Introduction To Seniors vs. Crime

In 1989, some of Florida's most effective citizen sleuths were unleashed through the creation of the Attorney General's Seniors vs. Crime project. This project, sponsored by the Office of the Attorney General, allows seniors to be actively involved in their own protection, as well as the protection of their fellow citizens.

Seniors vs. Crime has offices throughout the state of Florida staffed by volunteers, known as Senior Sleuths. The volunteers serve as the "eyes and ears" of the program and help ensure the Office of the Attorney General stays current on the issues affecting seniors. The volunteers also educate the public about scams and frauds; assist law enforcement, as requested; and manage and attempt to resolve informally consumer complaints involving seniors.

The Sleuths come from every walk of life and lend their experience and training to help those in need. The efforts of Seniors vs. Crime have resulted in the recovery of millions of dollars for seniors who were victims of con artists or dishonest businesses.

Get Assistance From Seniors Vs. Crime

Seniors vs. Crime is a non-profit 501(c)(3) organization that offers free assistance to seniors in need. Seniors who feel they have been taken advantage of in any financial dealing may file a complaint with Seniors vs. Crime at no cost. Should the organization be able to recover funds for the senior, the senior will receive every cent of that recovery. Seniors vs. Crime also offers speakers at no cost to educate senior and community groups on the program as well as typical scams and fraud directed at seniors.

Seniors may visit a Seniors vs. Crime office in person during office hours, file a complaint online at **www.SeniorsVsCrime.com** or call the toll-free hotline at ***1-800-203-3099***. Seniors who file a complaint online or through the hotline will be contacted by a Senior Sleuth in the nearest office.

Become A Sleuth

"Eyes and Ears Sleuths" are volunteers who do not wish to actively serve in an office but are willing to assist in special projects when called upon. These Sleuths determine the extent to which they wish to be involved. They may be called on to report on shopping experiences at a particular retailer, report instances of high pressure sales tactics or unfair trade practices or take on other similar tasks.

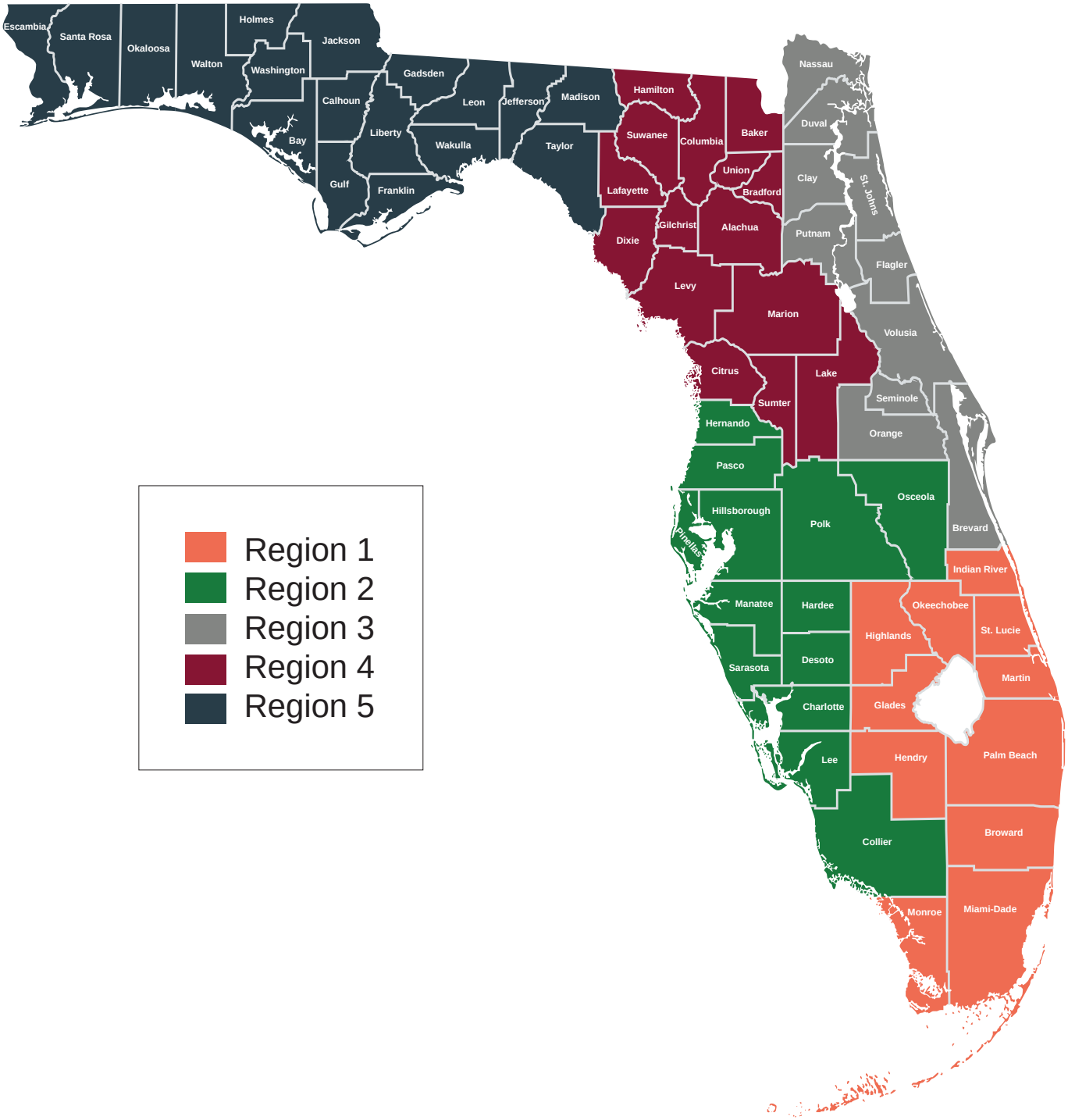
"Senior Sleuths" who wish to participate more actively may be trained to staff the Seniors vs. Crime offices where they record and work to resolve consumer complaints. They may also be trained to give presentations to groups regarding the Seniors vs. Crime program, its mission, current scams and crime prevention issues.

Sleuths with a financial background are also given the opportunity to present information about investment scams through the Florida Seniors Against Investment Fraud (FSAIF) program. Additionally, Senior Sleuths may opt to assist law enforcement by participating as actors in various "sting" operations. Unethical businesses and individuals may believe that their senior target is vulnerable, when, in fact, the senior may be working with the Office of the Attorney General or local law enforcement in an undercover role.

For more information about the Seniors vs. Crime project or to find an office location, visit **www.SeniorsVsCrime.com** or call toll-free at ***1-800-203-3099***.

*See the Seniors vs. Crime Regions map on page 26 to determine the region in which you are located.

Seniors vs. Crime Regions



PL-01 The Capitol
Tallahassee, Florida 32399-1050
(850) 414-3300
www.myfloridalegal.com