Protecting Ohio's Families

Senior Advocate Fraud Education (SAFE)

T O O L K I T

MIKE DEWINE
★ OHIO ATTORNEY GENERAL ★

www.OhioAttorneyGeneral.gov

About the SAFE Program

The Ohio Attorney General's Office, with support from the Sears Consumer Protection and Education Fund, has developed the Senior Advocate Fraud Education (SAFE) program to protect Ohio's families. Initiated by the office's Consumer Protection Section, SAFE educates caregivers, social workers, seniors, and their families about fraud and scams that target older adults.

Scammers use a variety of tactics to make their offers seem legitimate. The initial contact usually occurs by telephone, letters, door-to-door solicitations, fliers, e-mails, and/or phony websites. They often try to convince consumers to send money or give them personal information, such as bank account and Social Security numbers.

Consumers should know that scams come in many different shapes and sizes, but there is one common thread: Scammers all want to take money or personal information from consumers!

This SAFE Toolkit explores:

- Why older adults are targeted
- Scams that affect seniors
- Insurance fraud
- Safe investing
- Managing utility bills to prevent scams
- Identity theft
- Credit and debit card fraud
- Building and maintaining safe, fraud-free environments

Understanding Why Older Adults Are Targeted

Con artists and scammers often target older adults. According to one estimate, seniors represent 15 percent of the population but attract more than 30 percent of reported fraud.[1] Considering the likelihood that many incidents are not reported, the problem is probably far greater.

According to the Federal Bureau of Investigation, scam artists target older adults because of these common characteristics:

- **More trusting and polite:** Older adults are part of a generation that often based deals on trust and a handshake. Also, they may not want to appear rude, so they are less inclined to simply hang up the phone, even if an offer sounds too good to be true. They want to believe the other person.

- **Looking to bolster retirement savings:** Often retired and on fixed incomes, seniors may be especially vulnerable to "risk-free" investments. As a result, they may invest a great deal of money in an investment that promises high rates of return.

- **More assets:** The National Committee for the Prevention of Elder Abuse estimates that people over the age of 50 control more than 70 percent of our nation's wealth. They are more likely to have retirement savings, own their own home, and/or have excellent credit — and scammers know that.

- **May not report fraud**: Seniors are less likely to report fraud because they may not know who to report it to, may be ashamed, or do not know they have been scammed.

- **May be independent and/or isolated:** Living alone or far from family may make some older adults more vulnerable to scams and fraud. They may not have anyone with whom to discuss too-good-to-be-true investment offers.

Older adults, caregivers, friends, relatives, and neighbors of older Ohioans all play a crucial role in preventing fraud. Education and outreach are vital in this effort. By informing loved ones about topics covered in the SAFE Toolkit, consumers can help keep others from falling victim to scams. Reporting fraud to the proper authorities, including local law enforcement and the Ohio Attorney General's Office, is also important in protecting Ohio families from financial predators.

[1] Consumer Action (http://consumer-action.org/).

Persuasion Tactics

Scammers use many tricks and tools to persuade older adults to give them money and/or personal information. One common tactic is to impersonate a government official or falsely claim to be from a legitimate business or agency.

Among the people and organizations scammers may impersonate:

- Federal, state, or local governments
- Police departments or investigative units
- Courts, judges, or law firms
- Debt collection services
- Legitimate businesses, including major banks and corporations
- Charities (using the name of a real organization or one that sounds legitimate)

Scammers sometimes claim to be associated with a group to which an older adult may belong. They could, for example, pose as a military service member or veteran to try to persuade an older veteran to fall for a scam.

They also may use emotional ploys, build a sense of fear into their story, or prey on someone's need for money to scam seniors.

Scams Targeting Older Adults

Basic descriptions and scenarios can help Ohioans better understand today's common scams. However, it is important to note that fraudsters use many variations of these cons. Armed with savvy techniques and the latest technology, scammers are constantly finding new ways to swindle vulnerable people.

These scams and variations of them are common today:

Advance Fee Loans

In this ploy, scam artists trick consumers into paying money to qualify for a loan or credit card. Scam artists may "guarantee" a line of credit or promise to deposit money in consumers' bank accounts once they pay an initial fee. Despite these claims, however, consumers will not receive a loan, credit card, or any money. In general, consumers should never pay in advance to qualify for a loan or credit card. Also, they should be very cautious before applying for loans online, especially where other states' laws may not provide the same protections as those in Ohio. Some illegitimate lenders may conduct business online simply to steal consumers' money or to gain their personal information to commit identity theft or other fraud.

Credit Repair Scams

Credit repair scams involve false promises that bad credit can be erased, interest rates can be lowered, or debts can be consolidated. Many companies charge hundreds or thousands of dollars but do little or nothing to improve consumers' credit. In reality, they cannot erase accurate negative information from a credit report. With certain exceptions, negative information will remain on consumers' credit reports for up to seven years. If consumers want to improve their credit, they should contact a nonprofit credit-counseling agency or reach out to their creditors directly. They may be able to arrange a payment plan themselves at no or very little cost.

Fake Check Scams

Scammers use a variety of tactics to make fake check scams seem legitimate. A potential victim may receive a lottery "win notification" with a check enclosed. The notice instructs the victim to deposit the check and wire transfer money to cover taxes and fees associated with the winnings.

Scammers might also target individuals who advertise products in online marketplaces. For example, a scammer may contact someone who listed a vehicle for sale. The scammer will send a check for more than the car is advertised, and then instruct the seller to deposit the check and wire the difference.

Regardless of the pitch, the result is always the same: The scammer's check will fail to clear. As a result, the funds that the consumer thought were deposited into his account will not be credited, and the victim will lose any money that was debited out of his account.

Family, Caregiver, and Friend Scams

Sadly, family members, caregivers, and friends often are the offenders in many cases of financial abuse involving older adults. These trusted individuals may use credit cards without permission, manipulate victims to sign over power of attorney, and even forge the victim's signature. Consumers should watch for signs of a family or caregiver scam, including a senior's bills going unpaid, a new "best friend," excluding other family members or friends, unusual banking activities, or missing belongings. Seniors should be especially leery of those seeking to gain power of attorney over the individual, because this can provide full access to all financial accounts.

Foreclosure Rescue Scams

Foreclosure rescue scams target homeowners having trouble making their house payments. A phony foreclosure rescue company might contact individuals and promise to negotiate with their lender. Victims will pay thousands of dollars, but the company makes little or no contact with the lender. Consumers should never pay an advance fee for a loan modification.

In some cases, a phony "investor" may offer to buy the house and lease it back until the homeowner can afford the mortgage payments. The investor takes the money, but does not transfer the mortgage loan or pay the lender. As a result, victims risk losing equity and possibly their home. Consumers who are having trouble making mortgage payments should contact their lender directly rather than through a third-party company.

Grandparent Scams

In this scam, con artists call grandparents and pose as their grandchildren. They use an elaborate story to trick grandparents into sending money they think will benefit their grandchildren. The scammer may claim they are stuck in a foreign country and need money to get home. Or they may pretend to be an authority figure, such as a police officer, and threaten to keep the grandchild in jail until a "bond" is paid. Regardless of the pitch, the result is the same: Any money sent will be lost. When in doubt, seniors should ask the caller a question only a member of their family would know how to answer. Also, seniors should call their son, daughter, or another family member to confirm the location of their grandchild.

Healthcare Fraud

Many older adults have frequent contact with legitimate health care providers, but also may be targeted for scams. For example, a scammer posing as a federal government official may contact seniors, tell them they need to "update their records," or issue them a "new Medicare ID card." The scammer asks them to "verify" their Social Security number or other personal information, but instead of issuing a new card, uses the information to commit identity theft.

Seniors are also targeted with medical device scams. In one variation, a scammer tells a senior that family members have purchased a medical alert device on his behalf. Then the con artist asks for a credit card number to pay for shipping or monitoring fees. In reality, no family member purchased a device, and the scammer receives access to personal information.

The Attorney General's Medicaid Fraud Control Unit investigates allegations of financial exploitation involving residents of long-term care facilities as well as other potential offenses. When elderly or disabled adults are victimized, Ohio law allows for stiffer penalties for offenses such as theft, unauthorized use of property, misuse of credit cards, and forgery. For information about health care insurance fraud, see the separate "Insurance Fraud" section of this document.

Home Improvement Scams

This occurs when contractors or companies do little or no work for which they have been paid. Door-to-door contractors may offer to repair a consumer's roof, pave their driveway, or trim their trees for a good price. After being paid, however, the contractor disappears without doing any work or after doing a poor job. Scam artists may say they will give a consumer a discount or have leftover supplies from repairing another house in the neighborhood and therefore can offer a good deal. These false promises are tricks to steal a consumer's money. Consumers should beware of contractors who show up at their door. Current Ohio law requires that sellers give consumers a three-day right to cancel most door-to-door sales, and no work should begin before or during the three days.

Identity Theft

Identity theft occurs when someone obtains and uses a consumer's personal information, such as their bank account number or Social Security number, to commit a fraud. The thief may try to obtain credit, take out a loan, obtain medical treatment, get identification, or otherwise pretend to be the consumer. Identity thieves may open new accounts or purchase products in a consumer's name and then leave the consumer to pay the bill. To help prevent identity theft, consumers should never give personal information to anyone they don't know or trust. For additional information and methods to protect themselves, consumers should read the "Fighting Back Against Identity Theft" section of this toolkit.

Living Trust Scams

A living trust is a legal arrangement in which assets are transferred into a trust while the consumer is still alive, which keeps the assets from going through probate court when the consumer passes away. Trusts can be useful estate planning devices, but scam artists have been known to make exaggerated or false claims about probate costs or the tax advantages of living trusts. These scams usually target lower-income consumers, whose limited estates likely would incur minimal probate costs. Consumers considering buying a living trust should consider all their estate planning options and be wary of one-size-fits-all offers. They should consult an attorney for individual advice before signing contracts or making purchases. There also are legal aid programs that offer free help for seniors 60 and older regardless of

income. Consumers should hesitate to buy legal services from door-to-door salespeople, telemarketers, or online.

Phishing

Some scammers "phish" for personal information using cleverly designed phone calls or emails. They often pretend to be an employee of a consumer's bank or a government agency and ask a consumer to update or confirm their account information by submitting their bank account numbers, passwords, or Social Security numbers. Consumers should never respond to unexpected requests for personal information. Instead, they should return the call to a number they know to be associated with the company.

Phony Charities

Someone pretending to represent a charity may call or send a letter asking consumers to make a charitable donation. Consumers should always ask how much of their donation would actually go to the charity. Charitable organizations operating in Ohio are required to register with the Ohio Attorney General's Office. Before donating, consumers should verify that the charity is legitimate by calling the Attorney General's Help Center at 800-282-0515.

Prize/Sweepstakes Scams

Someone may fictitiously claim consumers have won the lottery, a contest, or a prize that they never signed up to win. To collect the winnings, however, consumers are asked to pay a fee. Often, they will be instructed to send money via wire transfer, money order, or prepaid money card, possibly to a foreign country. They'll tell consumers to expect their winnings once they pay, but the prize never arrives. Consumers should remember that legitimate sweepstakes are free and require no up-front payment. Also, it is illegal to participate in foreign lotteries.

Reverse Mortgage Abuse

A reverse mortgage is not necessarily a scam; it is a loan accruing interest that allows older adults to convert home equity into cash. However, some unscrupulous salespeople might pressure seniors into taking out reverse mortgages that have very high fees. Others tempt seniors to use money from the loan to buy annuities or investments that may not benefit them. Seniors should be cautious of taking out a reverse mortgage unless they fully understand all the costs, terms, and conditions. Seniors should keep in mind that reverse mortgages substantially reduce their home equity, and the total amount they owe on their home will grow over time.

Veterans' Benefits Misinformation

Some companies will offer information about veterans' benefits to gain seniors' trust. They may falsely imply that they work for the U.S. Department of Veterans Affairs (VA), make exaggerated claims about veterans' benefits, or encourage veterans to buy financial

products they don't need. For reliable information about VA benefits, veterans should contact their county Veterans Service Office.

Work-at-Home and Business Opportunity Ploys

Work-at-home and business opportunity ploys use sales pitches claiming that consumers can make good money by working from home or getting involved in a business opportunity. Consumers will be urged to pay in advance for materials or start-up costs. Ultimately, the only people who profit are the scam artists. Consumers should beware of seminars that promise money-making advice but deliver only high-pressure sales pitches. Consumers should also consider if the rate of pay reasonably matches the amount of effort required for the job.

Warning Signs of a Scam

Some signs that an "opportunity" may be a scam:

- You're asked to wire money or buy a prepaid money card for a stranger.
- You're told you've won a contest you never heard of or entered.
- You're pressured to "act now!"
- You have to pay a fee to receive your "prize."
- Your personal information is requested.
- A large down payment is requested.
- A company refuses to provide written information.
- A company has no physical address, only a post office box.
- Someone insists that you pay in cash.
- You receive a guarantee that you'll make money without any risk.

Always remember, if it sounds too good to be true, it probably is!

Managing Utility Bills and Avoiding Scams

Utilities — from electric and natural gas to telephone and water services — are essential services for Ohioans. These bills can also present some consumers with challenges when funds are tight. It is important that consumers contact their utilities and/or utility regulators if they are having financial difficulties and will have trouble paying their monthly bills. There are programs and payment plan options that may help consumers keep up with utility bills. The Public Utilities Commission of Ohio (PUCO) regulates investor-owned utilities in our state and has a hotline to help individuals with utility-related problems. The PUCO can be reached at 800-686-7826 or www.puco.ohio.gov. The Office of the Ohio Consumers' Counsel is the residential utility consumer advocate and can be reached at 877-742-5622 or www.occ.ohio.gov.

It is important to be aware that some instances of identity theft are related to telephone or utilities fraud. For example, a scammer may falsely claim a consumer will receive a grant to pay a utility bill in order to obtain personal information. In other cases, scammers may send fake utility bills to consumers' email accounts claiming that hundreds of dollars are owed. Another scam involves false claims that a utility account is past due. The scammer typically tells unsuspecting consumers they must pay the overdue amount through a wire transfer or prepaid money card to avoid a shutoff.

Consumers should take the following steps to protect themselves:

- Be skeptical of callers who threaten to shut off the power unless an immediate payment is made.
- If consumers receive a suspicious or threatening call, they should hang up and call their utility company using the telephone number on their monthly billing statement.
- Demand information in writing before sending any payment.
- Don't trust someone who says payment must be made using a prepaid money card or wire transfer. These are preferred payment methods for scammers.
- Keep all utility account numbers private unless a decision is made to switch to a new supplier. Once consumers have made a decision to switch, their new utility supplier will need their account numbers to process the change. Waiting to disclose the account number helps prevent "slamming," which is the switching of utility suppliers without a consumer's permission.

Insurance Fraud

One way of committing fraud or identity theft is by using someone else's insurance information. Consumers should closely review insurance statements and medical billing statements for procedures or other services they do not recognize. It is possible that someone used their personal information to receive treatment. To help prevent insurance fraud, consumers should not carry a Medicare or Social Security card in their wallet or purse unless they need it that day for an appointment. For additional information, consumers should read the "Closer Look at Insurance Fraud" box accompanying this section.

SIDEBAR: A Closer Look at Insurance Fraud

Insurance comes in several varieties (such as auto, home, health, life), and unfortunately, fraudsters often try to take advantage of older adults.

- With auto insurance, scammers may attempt to participate in phony accidents and claim physical injury. In the area of health insurance, scammers may file false claims, and some individuals in the medical field may provide and bill for unnecessary treatments. Fraud involving homeowners' insurance may entail a phony burglary along with claims for "stolen" goods or claims that homes need to be repaired when, in reality, they don't.

- Regardless of how it is perpetrated, insurance fraud is costly for insurance companies as well as for consumers who legitimately buy and use their insurance policies.

- Insurance companies in Ohio are mandated to have programs to help reduce fraud. In addition, the Ohio Department of Insurance's Fraud Unit investigates potential cases of fraud and can be reached at **800-686-1527** or online at **www.insurance.ohio.gov**.

- Annuities are insurance products that involve consumers making one or more initial payment and, in return, receiving those payments back over a period of time, perhaps for the rest of consumers' lives. While some annuities are legitimate financial instruments, consumers should be sure to scrutinize the costs and risks before signing a contract and investing any money. Costs can include fees paid to the salesperson or charges for surrendering the annuity early. In addition, older consumers may not live to take advantage of the perceived benefits.

Consumers should consider these tips regarding insurance:

- Stay home when contractors are inspecting the home. Otherwise, contractors could cause additional destruction to the property.

- Be leery about giving a power of attorney to contractors, even though the contractor may request a power of attorney to work with the insurance company.
- When purchasing life insurance or annuities, know all of the terms and conditions associated with the purchase, including payout terms.

Investment Fraud

Scammers might offer consumers a "risk-free" investment only to steal their money. For example, some scam artists convince consumers to invest in coins and precious metals, such as gold. Consumers should remember that all investments involve risk. They should research a company and consult with trusted family members or friends before making important financial decisions. For additional information, consumers can read "A Closer Look at Investment Fraud" in this section.

SIDEBAR: A Closer Look at Investment Fraud

Wouldn't everyone like to find an investment opportunity that will get them rich quick? Wouldn't it be great to get a double-digit rate of return with absolutely no risk? The truth is that these concepts are merely dreams, not reality. Investments always involve some risk, typically proportionate to the level of potential reward. Wise investing also may take years or even decades to produce successful results.

Here are several types of investment scams:

Affinity fraud: In these cases, a scammer tries to identify with someone's characteristics such as their ethnic background, occupation, religion, or hobby. For example, a veteran may try to build a level of trust with active military or other veterans. Once that trust is gained, the potential victim may lower their guard and be more vulnerable to an investment they might ordinarily think is just a scheme.

Ponzi or pyramid schemes: Many products, services, and investment instruments may help the seller and not the potential investor. Consumers should be leery of offers that appear too good to be true. For example, they should scrutinize claims of outrageous profits virtually overnight or pressure to act quickly without carefully evaluating the opportunity.

Promissory notes: These are essentially loans that investors make to a company with the promise that the investor will be paid in a certain timeframe with interest. Consumers should be wary of a potential scam if the person pitching the "investment" wants an immediate buy-in from the consumer, makes claims of no risk, or promises to make full payment back in a short period of time (such as nine months or less).

The Ohio Department of Commerce regulates many investments and can be a useful consumer resource. To find out if an investment or salesperson is registered, consumers should call **800-788-1194** or visit **www.com.ohio.gov/secu**.

The Ohio Department of Commerce reports these phrases are typical of an investment scam:

- “Your profit is guaranteed.”
- “It’s an amazingly high rate of return.”
- “There is no risk.”
- “You can get in on the ground floor.”
- “The offer is only available today.”
- “I’ll get you the paperwork later.”
- “Just make your check out to me.”
- “You would be a fool to pass this by.”

Fighting Back Against Identity Theft

Identity theft occurs when someone obtains and uses an individual's personal information without his permission in order to commit a fraud.

Examples of personal information to protect from identity theft are:

- Name
- Address
- Phone number
- Bank account number
- Credit card number
- PIN number
- Password
- Social Security number
- State ID card
- Driver's license/number
- Commercial driver's license number
- Birth certificate
- Place of employment
- Employee ID number
- Mother's maiden name

Knowing how thieves obtain personal information enables consumers to better recognize safe ways to keep and store it. In this age of information, criminals can easily acquire personal data about others. Some criminals pick through trash to find discarded documents containing personal information in a practice known as "dumpster diving," or use randomly selected Social Security numbers. Dishonest restaurant servers may secretly record credit card information when they take consumers' credit cards away from the table.

Phishing , Vishing, and SMiShing

Identity thieves also use the Internet to obtain personal information. In a popular scam known as "phishing," identity thieves hunt for a consumer's personal information by sending an e-mail message designed to trick the consumer into revealing sensitive information, such as account numbers, passwords, and Social Security numbers. "Vishing" occurs when the request originates via phone call or voicemail rather than email. For instance, a vishing message may instruct the recipient to call a toll-free customer service number that either logs keystrokes — such as account numbers — or connects the consumer directly to a scammer pretending to be a legitimate company. "SMiShing" is similar, but occurs via short message service (SMS) or text message.

Usually, all phishing, vishing, and SMiShing messages appear to be sent from a legitimate institution, such as a bank, an online payment service, or a government agency, such as the IRS. Often, the message asks the consumer to update, validate, or confirm account information by submitting sensitive personal information. However, banks and government agencies generally do not request personal information by email, text, or phone. If consumers fall for the scam, the scam artist captures their personal information, which they may use to commit identity theft.

Security Breaches

A security breach usually occurs when personal information is stolen from computers, back-up tapes, or patient records. If a consumer's information has been compromised in a security breach, it does not necessarily mean that his identity has been stolen. However, a security breach does increase the potential that the consumer's personal information could be misused. Consumers usually can avoid becoming victims of identity theft if they take action immediately after they discover their information has been compromised. They should contact their banks, place an alert on their credit reports, and take steps to protect their identity and consistently monitor their account activity.

You can take important steps to reduce the likelihood of identity theft:

- Check your credit reports at **www.annualcreditreport.com** at least once a year.
- Monitor your bank account and credit card statements regularly.
- Never carry unnecessary personal information in your wallet or purse.
- Shred documents containing personal information.
- If a billing statement fails to arrive, contact the company immediately. Thieves may steal information from mailboxes.
- Never share personal information with anyone who contacts you unexpectedly.
- Update your computer software and mobile applications regularly.
- Use Internet passwords that are hard to guess, and change them regularly.
- Set passcodes on your smartphone.
- If doing business online, make sure the site is secure. The Internet address should start with "https." The "s" indicates it is a secure website.
- Make copies of your credit cards (front and back) so you can call and cancel them quickly if they are lost or stolen.

Another step to consider is requesting a credit freeze from the three major credit reporting agencies. In Ohio, a credit freeze is permanent until the consumer asks for it to be temporarily or permanently lifted. Once credit is frozen, potential creditors cannot get the consumer's credit report so thieves are unable to open lines of credit. Consumers can still apply for jobs, refinance mortgage, buy insurance, or do anything that requires your credit report. If consumers want a business, lender, or employer to view their credit report, they can simply ask the credit reporting agency to lift the freeze. Freezing and thawing a credit report costs $5 per agency, or $15 for all three agencies, each time you do so.

Some signs you may be a victim of identity theft:

- You find inaccurate personal information or unfamiliar accounts on your credit report.
- Bill collectors contact you about debts you do not owe.
- You no longer receive certain mail or you receive mail related to unfamiliar credit cards.
- You are denied credit for no apparent reason.

Know the immediate steps to take if you become a victim of identity theft:

- File a report with your local police department or sheriff's office.
- Place an initial fraud alert on your credit report through one of the three credit reporting agencies:
    - Equifax, 800-525-6285 or www.equifax.com
    - Experian, 888-397-3742 or www.experian.com
    - TransUnion, 800-680-7289 or www.transunion.com
- Confirm that the agency you choose will notify the other two credit reporting companies that an initial fraud alert has been placed.
- Order your credit reports and contact your bank or credit provider.
- Contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioAttorneyGeneral.gov.

The Ohio Attorney General's Consumer Protection Section has an Identity Theft Unit to help victims rectify the effects of identity theft. Consumers who believe they have been the victim of identity theft should call the Attorney General's Office Help Center at 800-282-0515.

Avoiding Credit and Debit Card Fraud

Credit and debit cards are convenient for those who do not want to carry large sums of cash or who would like to make large purchases to pay over time. However, it is important to remember the risks associated with credit and debit cards, specifically fraudulent charges. Federal laws protect consumers, their credit and debit cards, and consumers' liability for fraud:

- **Credit CARD Act:** The Credit Card Accountability, Responsibility, and Disclosure Act (Credit CARD Act) of 2009 bans interest rate increases within the first year after a consumer opens a new account. It also bans a practice called "universal default," in which credit card companies could raise interest rates if consumers were late on other payments, such as cell phone or utility bills.

- **Electronic Fund Transfer Act:** This federal law addresses consumers' rights and banks' responsibilities related to debit card transactions. If a consumer's debit card is lost or stolen, it should be reported to the bank as soon as possible. If the consumer reports the loss within two business days, his liability is limited to $50 for unauthorized transactions. If the loss is reported within 60 days of receiving a statement containing unauthorized transactions, the consumer can be liable for no more than $500. Once a consumer notifies his bank, the bank must investigate the issue within 10 days. If the investigation takes longer than 10 days, the bank often must temporarily credit the customer for the amount of the disputed transactions. In total, the investigation must be completed within 45 days.

- **Fair Credit Billing Act:** This federal law gives consumers the right to dispute unauthorized credit card charges of more than $50 with their credit card provider. Because of this protection, it is often safer to pay with a credit card rather than a debit card. In order to dispute unauthorized charges on credit cards, consumers must send a letter to their credit provider (at the address given for "billing inquiries") so it reaches the creditor within 60 days after the first bill containing the error was mailed.

More credit card tips:

- Save all receipts and compare them with your credit card statements. If you find errors on your credit card statement, immediately contact your credit card company. Review your credit card statements regularly online. This will allow you to quickly identify improper charges.

- Exercise your right to opt out. The consumer credit reporting agencies allow consumers to choose to stop receiving credit card offers in the mail or via e-mail. “Opting out” can help reduce the risk of credit card fraud, because some identity thieves steal pre-approved offers to apply for and obtain credit in the victim’s name. To opt out of receiving these pre-approved offers, call 888-567-8688 or visit www.optoutprescreen.com. You can also tell your credit card company not to share your personal information with companies affiliated with your creditors.

- Do not give your credit card number to anyone you do not know or trust.

- Shred unwanted credit card applications so no one else will apply in your name.

- Check each of your three credit reports for free once a year at www.annualcreditreport.com. You will have to pay extra if you want to check your credit score. Do not fall for other “free credit report” offers that automatically enroll you in a costly monthly payment plan.

Building and Maintaining Safe and Fraud-free Environments

Consumers should protect themselves and beware of potential scams in their communities to help build and maintain a safe neighborhood free from con artists. These important tips can help consumers stay safe:

- **Research businesses and charities:** Before doing business with a company, consumers should check its reputation with the Ohio Attorney General's Office at **www.OhioAttorneyGeneral.gov** and the Better Business Bureau at **www.bbb.org**. Consumers should ask family and friends for recommendations and never pay money to a person or company that refuses to give them written information, a phone number, a physical address, or references. Consumers should consider conducting an online search to find reviews about the business or charity, too.

- **Read the fine print.** Consumers should read all the terms and conditions of any agreement and review contracts with a trusted attorney, friend, or family member before signing. If a fraudulent charge appears on a bank or credit card statement, consumers should immediately notify their bank.

- **Get warranties and all verbal promises in writing.** If it is not in the contract, it is not a guarantee. No detail is too small to ask to put into a contract.

- **Remember consumer rights.** Ohio consumer laws protect Ohioans from unfair, deceptive, and unconscionable practices in consumer transactions. For example, advertisements must list exclusions, limitations, or conditions of the offer, and a store must clearly post its return policy.

- **Reconsider the purchase.** Don't give in to high-pressure sales tactics. If it's a "good deal" today, it should be a good deal tomorrow, too. In Ohio, most door-to-door sales must come with a three-day right to cancel, which allows you time to reconsider your purchase.

- **Report scams and unfair practices.** If a consumer has a problem with a purchase, he should notify the company in writing. If the consumer is unable to resolve the complaint, he can file a complaint with the Attorney General's Office and state a desired resolution. The Attorney General's Office also accepts complaints about scams.

Even with the widespread use of email, phony websites, and social media, many scams begin with a telephone call from the scammer to the victim. Consumers should know how to handle unwanted phone calls to reduce the risk of being scammed:

1) **Do not trust caller ID**. Spoofing technology allows scammers to disguise their true identity and the origin of their phone calls. They can make it appear that a call is coming from a local bank, when it actually is coming from some other country. They often achieve spoofing by using Voice over Internet Protocol (VoIP), technology that allows individuals to make telephone calls using the Internet.

2) **Think before giving out a phone number**. Consumers should think twice before responding to a request for their phone number. Companies may compile and sell this information to other companies that may be interested in soliciting the consumer. Also, this information may end up in the hands of scammer.

3) **Opt out of sharing your personal information**. Many businesses automatically share personal information with other businesses. Consumers can take active steps to "opt out" of having their information shared. Consumers should not provide credit card numbers or bank account information over the phone unless the consumer initiated the call.

4) **Do Not Call**. Consumers can reduce unwanted telemarketing calls by registering with the National Do Not Call Registry by visiting **www.DoNotCall.gov** or calling **888-382-1222**. There are certain exceptions to the Do Not Call Registry, including charities, political organizations, survey companies, businesses with which you have a pre-existing business relationship, and businesses to which the consumer has submitted an inquiry.

Resources

Attorney General's Office
800-282-0515
www.OhioAttorneyGeneral.gov

Better Business Bureau
www.bbb.org

Federal Trade Commission
877-FTC-HELP
www.ftc.gov

Do Not Call Registry
888-382-1222
www.donotcall.gov

Opt Out Prescreen
888-567- 8688
www.optoutprescreen.com

Annual Credit Report
877-322-8228
www.annualcreditreport.com

Public Utilities Commission of Ohio
800-686-7826
www.puco.ohio.gov

Office of the Ohio Consumers' Counsel
877-742-5622
www.occ.ohio.gov

Ohio Department of Insurance
800-686-1527
www.insurance.ohio.gov

Senior Advocate Fraud Education (SAFE)

T O O L K I T

Consumer Protection Section
30 E. Broad St., 14th Floor
Columbus, OH 43215

800-282-0515

www.OhioAttorneyGeneral.gov

MIKE DEWINE
★ OHIO ATTORNEY GENERAL ★