THOMAS J. MILLER
ATTORNEY GENERAL

1305 E. WALNUT ST.
DES MOINES, IA 50319
Main: 515-281-5926
www.iowaattorneygeneral.gov

IOWA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

Consumer Protection Division

The Attorney General's Consumer Protection Division protects Iowa consumers from fraud, ensures fair competition in the marketplace, and informs the public about consumer frauds and how to avoid becoming a consumer fraud victim.

The Division enforces laws that protect the buying public from false or misleading advertisements or sales practices. It also enforces laws that help ensure consumers get information to help them make important decisions.

Mailing Address
Office of the Attorney General of Iowa
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319-0106

Website
www.IowaAttorneyGeneral.gov

Phone
515-281-5926
888-777-4590 (outside of the Des Moines metro area)

Email
consumer@iowa.gov

Fax
515-281-6771

Contact:
Al Perales, Investigator
515-281-6413
aperales@iowa.gov

Paying a Debt with an iTunes Card? Sounds Like a Sad Song!

Imagine pulling up to a highway toll booth and the attendant demands that you pay right now using an Apple iTunes, Amazon or PayPal gift card. That doesn't sound right, does it?

Of course not, and the same goes for anyone who calls you and demands immediate payment using a gift card. Scammers also demand money through prepaid reloadable money cards (such as GreenDot, MoneyPak or Vanilla), or wire transfer payments (such as MoneyGram or Western Union).

Scammers who seek payment this way are, in a sense, asking you to leave an electronic cash box on a virtual table. Once you provide a card's code or you wire money, you've given someone the key to that cash box and you probably can't get your money back once they've taken it.

Never provide gift card or prepaid money card information, or wire money, to anyone you don't personally know—even if the story sounds convincing.

The Most Common Scams

- **IRS Scams:** If someone calls unexpectedly claiming he or she is with the IRS, and threatens you if you don't pay immediately, it's a criminal calling. The IRS will contact you about debts or penalties through the mail—not the phone—and won't demand immediate payment through a money card, gift card, or wire transfer.
- **Tech Support Scams:** A caller claims that somehow your computer has been identified as the source of a virus, and he or she can fix it now. By allowing the caller to remotely access your computer to "fix" the problem in exchange for immediate payment by phone, it could result in your computer's data getting damaged or destroyed--not to mention the money you lost in the process.
- **"Grandparent" Scams:** A frantic caller will try to convince you that he or she is a relative, government official, or even defense lawyer, claiming that there's been an accident, incident or emergency. The caller seeks immediate payment over the phone. No matter how bad or legitimate it sounds, take the time you need to check out what's very likely a phony story. Ask personal questions that only your loved one would know. Try to contact other family members, a close friend, or even law enforcement to help you.

If you just provided card information or wired money and realize you may have been scammed, report it immediately.

- If you provided card information, contact the card provider.
- If you wired money, report suspected fraud to Western Union's fraud hotline at 1-800-448-1492, or MoneyGram at 1-800-MONEYGRAM (1-800-666-3947).

Unfortunately, it may be too late to stop or reverse the transaction, but it is worth every effort. You should also file a police report, and file a complaint with the Federal Trade Commission (FTC) at www.FTC.gov. You can also file a complaint with the Attorney's Consumer Protection Division.

Phone Seller Wants Quick Electronic Payment? No!

Thanks to a change in federal rules, beginning this month fraudulent telemarketers have fewer ways to take money away from your wallet or bank account, and consumers have greater protections.

The new restrictions target telemarketing fraud by banning certain payment methods that don't carry the types of protections for consumers that are guaranteed with credit cards and debit cards. These payment methods are often used by scammers and shady telemarketers who don't conduct business aboveboard.

Under the new changes to the Telemarketing Sales Rule (TSR), telemarketers are prohibited from accepting funds through these payment methods:

- **Wire Transfer:** This is a "cash-to-cash" money transfer, through services such as Western Union and MoneyGram. When a consumer pays for a wire transfer, the funds are loaded into a worldwide system and picked up by the recipient as cash. Once the transaction is complete, the money is gone—just like cash. Criminals try to convince their victims to wire money to a stranger, and the money often ends up in a foreign country.
- **Reloadable Prepaid Card:** This is commonly referred to as a prepaid money card or prepaid cash card. A consumer generally pays a service fee to obtain and activate a one-time use or reloadable card, and then load funds onto the account. Criminals seek a card number and Personal Identification Number (PIN) from consumers, and then transfer the funds out of the consumers' prepaid card accounts. While these cards seem similar to credit cards, they do not carry the same protections--they are much more like cash.
- **Remotely Created Check:** A remotely created check (RCC) is also known as a demand draft. With a demand draft, a consumer is supposed to give a merchant permission to withdraw funds directly from his or her checking account without a signature. In other words, it's an approved payment transfer from one bank account to another. A criminal may seek to trick a victim into providing account information over the telephone or the Internet.
- **Remotely Created Payment Order:** A remotely created payment order (RCPO), also called an electronic check, or eCheck, is an electronic version of a remotely created check. It poses many of the same risks posed by remotely created checks when scammers are involved.

The rules are designed to reduce the options for scammers to arrange counter-to-counter cash transfers or directly access bank accounts for withdrawals.

The rules don't change how consumers may use these payments for legitimate, routine transactions, such as consumers authorizing online payments from their bank accounts. These payment methods are not what reputable telemarketers use to do business.

General Advice

Criminals and dishonest sellers who don't play by the rules will come up with any kind of story to convince you over the phone to pay them. And they may try to rush or even threaten you.

- Buy only from reputable sellers that you are familiar with.
- Do not rush into anything. Take the time you need to consider it, ask for written information, do research, and think about asking for advice from someone you trust.

- Callers can easily manipulate your caller-ID display to block your display or show any phone number or listing they want —even your own name and number. Those same callers may provide false information about their names, who they represent, and why they are calling.
- Be wary of a caller who seeks payment through any of the methods listed above (such as a wire transfer, prepaid card, etc.).
- Avoid paying by gift card. No legitimate business will ask you to pay in gift cards.
- If you purchase something by phone, a credit card offers you the best protections and enables you to dispute fraudulent charges.

Dietary Supplements | Iowa Attorney General

Dietary Supplements

When you pick up a prescription medication, it's likely a drug that's been clinically tested, is proven safe, and is regulated by the U.S. Food and Drug Administration (FDA). When you purchase a dietary supplement, it's a product that the FDA does not evaluate or review for safety and effectiveness. That's because federal law treats supplements more like foods than prescription or over-the-counter drugs. In other words, the FDA is responsible for taking action against a dietary supplement product only after harm occurs. (Some manufacturers submit their products for third-party testing through independent laboratories such as the U.S. Pharmacopeia, or USP.)

What are Dietary Supplements?

Dietary supplements include vitamins, minerals, herbs and botanicals, amino acids, extracts, concentrates and metabolites. They are offered as tablets, capsules, liquids, and powders. Sellers may claim their products provide certain nutritional benefits, help you lose weight, boost energy, build muscle mass, relieve pain, slow or "stop" the aging process, or even prevent, treat or cure certain diseases.

Are they Good for Me?

Although supplement marketers often promote their products a vital to good health, supplements shouldn't replace a healthy, balanced diet. You may not need supplements if you maintain a good and varied diet, and too much of some nutrients (such as through vitamins) can cause problems. On the other hand, there are people who will benefit from some types of supplements — such as pregnant women who take folic acid.

But, as largely unregulated products, supplements may contain ingredients not listed on the product label; contain ingredients at higher or lower amounts than listed (or not even contain a listed ingredient); could be manufactured inconsistently; sellers may make false, misleading or unsupported "miracle cure" health claims; and some products may lead to serious health effects or even death. Unlike with drugs, supplement manufacturers are not allowed to promote their products to treat, diagnose, prevent, or cure diseases.

Mixing prescription medication with dietary supplements or mixing supplements alone could cause unintended side effects. Combining the two could strengthen, weaken, or even change how a medication or supplement affects you.

But Supplements are Natural Products, Right?

While a supplement manufacturer may market a product as "natural" and the product may, indeed, contain natural ingredients, even some natural ingredients can adversely impact your body and could, in certain situations, be unsafe.

Where Do I Turn to for Reliable Information?

Check with your health care provider before taking a supplement. Make sure your provider understands what you are taking, including the amount, and any other prescription medications, over-the-counter drugs, or supplements. Let your provider know if you are pregnant or nursing, whether you have any diseases or chronic conditions (such as cancer, heart or breathing problems, diabetes, high blood pressure), and whether you're about to have surgery. Ask about the potential benefits and risks of taking the supplement, just as you would ask about taking a prescription drug. If you are considering a

supplement for a child, check with the child's health care provider first.

If you search the Internet for information about a supplement, be aware of the source. For example, weigh the value of information you'll find on an established government, academic or reputable health-related website, versus information or testimonials posted on a site designed to market products or promote an industry.

What if There's a Problem?

If you think that a supplement has caused an adverse side effect, reaction or illness, report it to your health care provider and to the FDA. You can call 1-800-FDA-1088 to request a report form or file an online complaint at www.fda.gov. If you think that an advertisement about a supplement includes false health claims, contact the Federal Trade Commission at 1-877-382-4357 or file an online complaint at www.ftc.gov/complaint.

These Chips are Good for You

New Credit and Debit Card Chips

"Would you like me to swipe your credit card?" is a phrase whose days may be numbered.

Major card issuers are adding a small metallic square to new cards, which are computer microchips designed to enhance the cards' security.

This technology is what the electronic payment industry calls EMV, which stands for Europay, MasterCard and Visa. EMV is a global standard that establishes the payment transaction roadmap for cards with chips. Other countries have used this technology for years, but many U.S. consumers are just now seeing it.

And you're seeing it because card issuers and retailers have shifted liability when card fraud occurs. Whichever party has not upgraded to the newer chip technology will be held responsible for losses associated with card fraud. So card issuers are issuing new chip cards and merchants are upgrading their systems to minimize potential card fraud costs.

New Chip Technology Makes Cards More Secure

When you use a new generation credit or debit card embedded with a microchip, the chip creates a unique, one-time security code for each transaction. The enhanced security makes it more difficult for criminals to steal your credit card information from point-of-sale terminals.

Over the past several decades, cards have utilized a magnetic stripe on the back of each card. The magnetic stripe contains cardholder, account number and security code data, which always remains the same. A criminal can "skim" this data from point of sale terminals, through a hidden device or software that copies credit or debit card information from the magnetic strip when you swipe the card. With that data, criminals can use the card's information for remote fraudulent transactions or even create a duplicate card and use it just like the original card.

If you are a card user with a chip-enabled card, you'll have to get used to a new routine when paying with plastic at most point-of-sale terminals. Instead of swiping your card, you'll put it into a card reader slot and wait for transaction approval. Depending on your card's verification method, you may have to sign your name or enter a Personal Identification Number (PIN).

What won't change is how you use your card when paying by phone or through a website. That means that cards are still vulnerable if a criminal gets access to the data on your card. You should continue to protect your credit card information and always look for fraudulent activity by reviewing your financial statements.

Rollout Underway

It will take time for many retailers to transition to new systems, and most payment system agreements extend the deadline for upgrading gas pumps and automatic teller machines (ATMs) to next year. While the transition is underway, cards will contain both a magnetic stripe and computer chip. Unfortunately, the chip's enhanced security benefits don't factor in when using the traditional magnetic stripe.

Don't worry if you have not yet received a newer generation credit or debit card with a chip. It's possible your card issuer is waiting for your current card to expire, or may not have yet begun its replacement rollout. If you would like to know about the card replacement schedule, contact your issuer.

Whether you're using a credit card's chip or magnetic stripe to complete a transaction, keep in mind that it's still generally safer than paying by cash or check. That's because a credit card offers you certain protections and allows you to dispute a charge if goods or services are unfulfilled, or a charge was fraudulent.

Tax-Related Identity Theft and Refund Fraud

Tax-related identity theft and fraud are growing problems that state and federal revenue collectors are addressing this tax season through increased vigilance and safeguards.

Tax-related identity theft occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund. An identity thief will use your Social Security number to file a false tax return early in the year, and collect a refund.

You may be unaware you are a victim until you try to file your taxes and learn that a return has already been filed using your Social Security number. You may receive a notice that you owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return. You may also learn that IRS records indicate that you received wages from an employer unknown to you.

To help combat fraudulent tax returns, refunds and prevent tax-related identity theft, the IRS and Iowa Department of Revenue are asking taxpayers to be aware of the problem and take precautions to help prevent and identify it.

Changes for Online Filers

The IRS and state revenue agencies, including the Iowa Department of Revenue, are making changes to enhance security. You may notice some of these changes if you file your taxes online. The changes include new security requirements when you sign in to your account. In some cases, taxpayers may receive a refund check through the mail and not through a direct deposit as requested, to assure that refunds go only to the intended taxpayer and not a criminal.

Other Changes

Tax return preparation firms, tax preparation software providers, and other tax industry participants are enhancing certain security requirements and strengthen validation procedures. The changes include new password standards, security questions and other verification procedures.

Federal and state revenue agencies are enhancing their electronic monitoring of tax return submissions that will assist in preventing identity theft returns. For example, government computer systems will seek to detect improper or repetitive electronic addresses from where tax returns were transmitted.

Always protect your personal information

Do not routinely carry your Social Security card or documents that list the number for your or your dependent family members. Don't give a business your Social Security number just because they ask—only provide it when absolutely necessary. Shred sensitive documents before throwing them away.

Reporting Tax-Related Identity Theft

If you suspect you have been victimized by tax-related identity theft, report it:

- IRS Identity Protection Specialized Unit: 800-908-4490 or www.irs.gov
- Iowa Department of Revenue: https://tax.iowa.gov, or call 515-281-5986
- Call one of the three major credit reporting agencies to put a fraud alert on your credit report:

- TransUnion 800-680-7289; Equifax 800-525-6285; Experian 888-397-3742

- File a complaint with the Federal Trade Commission (FTC) at www.IdentityTheft.gov or call 877-438-4338
- File a report with your local police department or sheriff's office

Caller ID Spoofing | Iowa Attorney General

Caller ID Spoofing

Caller identification, or caller ID, is a telephone feature that enables the recipient of a call to see the caller's phone number and name displayed before answering the phone. While caller ID can help you screen unknown or unwanted calls, callers can easily manipulate your display to show incomplete or false information--even your own name and phone number. The technique is called spoofing.

Why They Do It

Criminals who spoof caller ID hope the displayed information will help convince you of their false identity and story. Others may spoof your caller ID simply to increase the likelihood that you'll answer the phone. The calls can come from individuals or robo-calling systems. For example:

- IRS Scam: A criminal, from anywhere in the world, can spoof your caller ID display to show an actual or fake Internal Revenue Service (IRS) listing. The caller claims he or she is with the IRS and you must pay back taxes immediately to avoid arrest or some type of imminent legal trouble.
- **Tech Support Scam:** A scammer can manipulate your caller ID display to show an actual or fake computer support listing. The caller claims that an Internet trace has determined that your computer is infected with a virus. The caller urges you to allow remote access your computer to fix the supposed problem for a fee.
- **Grandparent Scam:** Your caller ID device may falsely display a law enforcement agency, attorney's office, hospital, or a cell phone. The caller claims that he is your grandchild or is calling on behalf of your grandchild. The pretext of the call is that your grandchild is in trouble and needs immediate funds.
- **Identification Theft Scams:** These can take many forms. The caller may claim that he or she is with your financial institution or even law enforcement and is investigating a fraud case. The caller seeks personal financial information (such as account or credit card numbers), personally identifying information (such as your mother's maiden name), or passwords.
- **Sales and survey calls:** The caller may spoof your caller ID device to display false or incomplete caller ID information, or even your own name and number, to increase the likelihood that you'll answer the call. The call may be a sales or survey call.

How They Do It

Spoofing services are readily available for robo-calls or individual calls. They allow the caller to enter in any information—including any name and any phone number—to appear on the recipient's caller ID display. The calls, which can be placed from anywhere in the world, can be difficult, if not impossible, to trace.

Is Caller ID Spoofing Legal?

The federal Truth in Caller ID Act prohibits callers from deliberately spoofing caller ID to display inaccurate information with the intent to defraud, cause harm, or wrongfully obtain anything of value. There are some exemptions, however, for law enforcement agencies and situations where courts have authorized caller ID manipulation.

Telemarketers must display their own phone number or the phone number for the seller on whose behalf the telemarketer

is calling.

How to Handle It

Do not provide personal information to a stranger who calls, regardless of what appears on your caller ID display. To ensure you are not dealing with a criminal posing as someone else, hang up and place your own call. Look up the number of the entity that supposedly called you from a known source such as a phone book, invoice, or known website. If you are having trouble locating the information, ask someone you know and trust to help you.

How to Report It

If you receive a call from a telemarketer without the required information or suspect that a person or entity has illegally spoofed your caller ID display, you can report it to the FCC at www.fcc.gov or call 888-CALL-FCC (888-225-5322).

Health Plan Enrollment & Scams | Iowa Attorney General

If you're looking for health insurance coverage, look out as well for health care scams. Comparing health insurance plans during the open enrollment period can be confusing and raise lots of questions. Scammers and criminals take full advantage of this.

Consider Your Options

Before enrolling, review your current plan, if you have one, and decide whether it still fits your budget and the health needs of you and any other family members enrolled in the plan. As you compare your current plan with new options, think about the kinds of health needs that you and your family members are likely to encounter in the next year.

Finding Answers

If you have job-based insurance, talk with your employer about your options, costs and deadlines. Iowans seeking policies through the Health Insurance Marketplace can review them at www.healthcare.gov or call 800-318-2596. You may even qualify for savings based on your income. At www.healthcare.gov you'll find "navigators," who can help you apply for coverage and enroll you in a health plan. Navigators are trained and certified to provide health plan information that is fair, impartial, and accurate -- all at no cost to you.

Licensed insurance agents are trained and registered professionals who can also help you apply for coverage and enroll in a health plan. Their services are free, but remember that agents may sell only for certain health insurance companies.

Health Plan Enrollment Scams

Scammers may attempt to sell you plans that you don't need or coverage that is worthless. Criminals may attempt to steal personal or financial information under the guise of establishing or "confirming" a health care plan on behalf of the government or a company, or by offering "free" medical supplies or exams in exchange for your information.

Also, avoid government look-alike and imposter websites. These sites, whose website addresses do not end with ".gov," may connect you with salespeople or scammers, but not the official Marketplace.

Don't Provide Personal Information to a Caller

Medicare employees will not call you and ask for your Medicare number, Social Security number, or personal financial information. Anyone who calls and claims that they represent Medicare and asks for this information is not legitimate. Hang up the phone and contact Medicare at 1-800-MEDICARE.

Be wary of anyone who calls and claims that you will lose your Medicare coverage if you don't join their prescription plan. The Medicare prescription drug plan, also known as Medicare Part D, is voluntary and does not affect your Medicare Part A and B coverage.

Health Discount Plans

Finally, be wary of "health discount" or "medical discount" plans. With these plans, you generally pay a monthly fee to get purported discounts on specific services or products from a list of providers. Medical discount plans and limited benefit

plans don't pay your health care costs and don't meet the federal requirements of health insurance coverage.

While there are legitimate health discount plans, there are also plans that are of little or no value. Some sellers may make it sound like they're offering health insurance plans. Others may lie about their plans' coverage and costs. If it sounds too good to be true, it probably is. Before purchasing, get help from a trusted source like a licensed insurance agent or the Senior Health Insurance Information Program (SHIIP) at 800-351-4664.

Our office is a part of the Iowa Fraud Fighters team, in a partnership with the Iowa Insurance Division, the Iowa Department on Aging, and SHIIP, which provides Iowans resources about insurance scams and investment frauds at www.iowafraudfighters.gov. If you think you were targeted or victimized by an insurance scam or investment fraud, contact the Iowa Fraud Fighters team through the website or by phone at 877-955-1212.

Protecting Our Service Members and Veterans

Special consumer protection advice for the special Iowans who serve or have served in our military

Iowans who bravely serve our country through the active military, the National Guard or Reserves, military veterans who served, and their families, can get singled out by scam artists and disreputable businesses.

Active duty service members are sometimes targeted because of their reliable income and their likelihood to relocate or deploy. Bad actors people take full advantage of service members who fear that reporting a financial problem—even if it was the result of deception, fraud or unfair practices—may affect their military career.

Veterans can be targeted through VA benefits or pension scams, investment scams and dubious "special offers for vets only."

Scams Affecting Active Duty Service Members and Families

- **Military Paycheck Allotments:** Some of the most common scams that have traditionally affected active duty service members are those that sought to tap directly into military paycheck allotments, or designated amounts of money that are automatically distributed to a service member from his or her pay.

  Unscrupulous lenders would abuse the allotment system by selling, establishing rental or lease agreements, or extending loans with service members and their families for items such as vehicles, electronics, appliances and furniture. The merchandise would be offered at high prices, or the seller/lender would impose unreasonable and perhaps even illegal terms, fees and interest rates.

  Recently, for their protection, the U.S. Department of Defense prohibited service members from setting up allotments for personal property. But service members can still use allotments for uses including financial account deposits, investments, dependent support, insurance premiums, mortgages, rents, Combined Federal Campaign (philanthropic) contributions, and U.S. government debt repayments.

- **Payday Loans and Cash Advances:** Payday loans and cash advances are generally associated with high interest rates and fees. A consumer credit lender cannot charge service members (including National Guard members on national duty) or their families an annual percentage rate higher than 36 percent. These include payday loans, car title loans (which are illegal in Iowa), and refund anticipation loans.

- **College Loans:** Some for-profit schools may be more interested in seeking GI Bill payments than seeing that a service member receives the education he or she needs for a particular career. While all prospective students need to do plenty of research before enrolling in a higher education institution, service members need to be particularly vigilant. Some for-profit colleges have aggressively and deceptively recruited service members and veterans to enroll in high-priced, low-quality programs. The U.S. Department of Veterans Affairs provides helpful information at www.benefits.va.gov/benefits, and the U.S. Department of Education's College Navigator provides helpful information at

https://nces.ed.gov/collegenavigator.

Scams Affecting Veterans

- **Pension Advance Products & Pension Scams:** These are offers for "free help" with pension-related paperwork, or lump-sum payment offers to military veterans. In some cases, a veteran might receive a large up-front payment, but in the end may receive only a small amount of what he or she would have earned had they waited to receive full pension payments. In other cases, unscrupulous brokers, insurance agents, attorneys or financial planners may convince veterans to sign up for benefits that may cause them to lose eligibility for Medicaid services or cause other long-term financial setbacks. Never give a creditor access to the account where your benefits are deposited.

- **"Special Deals" for Veterans:** While some patriotic businesses truly want to thank veterans for their service through special offers, others may try to take advantage of them. Whether it's a loan, rental or purchase, veterans should research any "special deal" for vets before committing.

Grandparent Scam | Iowa Attorney General

Grandparent Scam

March 2015

It's one of the most heartbreaking scams that Iowans report to the Consumer Protection Division. A criminal exploits an elderly person's unwavering love, caring and instinct to help a grandchild or young relative in need. By claiming that he is a grandchild or a relative in serious trouble and needing immediate financial help, the caller tricks his elderly victim into letting down his or her guard. The Grandparent Scam has been around for several years but continues to target older people across Iowa and across the country. Some victims have lost tens of thousands of dollars.

The Surprise Call

You answer the phone to a distraught-sounding caller who refers to you as "Grandma" or "Grandpa." Unsure who it is, you respond with the name of your grandson, and the caller tries to convince you that it's really him. Or maybe the caller already knew your grandchild's name because he found it posted on a Facebook page or somewhere online.

The Surprise Claim

The "grandson" claims he's in another country and has landed in some sort of trouble. The story can include a car accident, an arrest, a mugging, or an emergency medical situation. The caller may even put others on the line who identify themselves as law enforcement officers, attorneys, bail bondsmen or medical professionals.

Not a Surprise: The Caller Wants Money Now

A Grandparent Scam caller always claims an emergency need for money, insists that you to need to act quickly, and pressures you to keep it quiet.

The criminal will try to convince you to wire the funds or deposit money into a prepaid money card account. That enables him to almost instantaneously receive a large amount of cash anywhere in the world, and the transaction may be impossible to stop or trace. He'll want you to act quickly so you don't take time to check out the story. And he'll insist that you keep this situation to yourself or might give you suggested responses should someone ask about the large transaction. The criminal knows that anyone who learns about the circumstance will try to stop it.

The Best Prevention is Communication

If a caller claims he needs emergency money--no matter who you think it is and what he tells you--do not act immediately to acquire and send money, do not be ashamed about asking questions, and do not keep it a secret. If the caller claims he is your grandson, ask him a personal question that only he would know (for example, ask about a pet, a previous vacation or an allergy). Ask the caller for his contact information, or better yet a public number like a police station, hospital or hotel, and let him know that you will get back to him soon. If it's truly your grandson, he'll provide you needed contact information. If it's someone else on the phone, he or she should be able to provide a number you can find listed on the Internet. Call your local police department or sheriff's office, as law enforcement can verify the story. Contact another family member (such as a parent or sibling of the grandchild) or someone you trust, and ask that person to help you.

If you have an older relative who could fall victim to the Grandparent Scam, discuss it with them. Make sure they have your

current contact information and inform them if you travel abroad. Be sure they understand the pitfalls of posting personal information online.

If You've Been Scammed

Unfortunately, these scams almost always lead to unrecoverable losses because wiring money is like sending cash. If you think you've been victimized by a wire fraud, contact the wire transfer company immediately. If the criminal has not yet picked up the cash, it may be possible to stop the transaction. Report the incident to your local law enforcement agency. You can file a report with the federal Internet Crime Complaint Center at www.ic3.gov, and you can also report it to the Attorney General's Consumer Protection Division.

First You Win, Then You Lose

january 2014

Prize, sweepstakes and international lottery scams

This must be your lucky day! Even though you didn't enter any drawing, you've been notified that you won something big—perhaps cash or a prize. All you have to do is pay some sort of processing or handling fee, advance taxes or entry fee, and it's all yours.

It'll be your unlucky day if you send any money. If someone asks you to pay in advance, wire money after receiving a "winnings" check, disclose account information, or buy something to better your chances of winning, it's a scam.

Don't Pay to Collect Prize

Legitimate sweepstakes and contests don't cost money to enter, and don't seek advance payment from winners to collect winnings. If you receive a check and someone asks you to send money through a wire transfer service, it is likely an international scam. The check may appear legitimate—even to a financial institution—but will eventually bounce. If you wired money to someone while waiting for the check to clear, which could take weeks, you're responsible for the money you wired. And as soon as someone picks up the wired funds, the money is gone.

Purchases Don't Push the Odds of Winning

It's illegal to specify or even suggest that a purchase will increase your odds of winning something. Those who conduct or market a sweepstakes contest must disclose that entering is free, no purchase is necessary, and must disclose the odds of winning a prize. Further, they must indicate the nature and value of the prize. The sweepstakes disclosure should also include information about the start and end dates of the contest, and how contestants can enter. Be sure to look for this information in writing.

International Lottery Scams

International lottery scams appear through email, direct mail and phone calls. The interstate or international sale of lottery tickets by mail or by telephone violates state and federal laws. There is no guarantee that a foreign lottery solicitor is actually entering lotteries on your behalf—these are often straight scams to take your money. It's possible that solicitors who ask you to pay through bank account or credit numbers will steal funds or make unauthorized charges from your account.

Protect Personal Information

If someone asks for personal information such as a driver's license or Social Security number for "tax purposes," don't provide it, as you will pay taxes directly to the government or the sweepstakes company will withhold the appropriate taxes on winnings. Most companies will seek nothing more than basic information such as your name, address and telephone number. And no legitimate company will ask you for bank account or credit card numbers.

Do a Little Research

Use a familiar Internet search engine to research a company that claims you won something. In addition to entering the company name into a search engine, add the word "scam" or "complaint" to see what comes up. If you're not comfortable doing the research, ask someone you trust to help you.

Consumer Protection Complaint Form

Tom Miller
Attorney General of Iowa
Phone: 515-281-5926
Fax: 515-281-6771
888-777-4590 (toll free, outside of Des Moines)

Consumer Protection Division
1305 East Walnut
Des Moines, Iowa 50319
Email: consumer@iowa.gov
www.IowaAttorneyGeneral.gov

Instructions:

1. Please print or type. Answer all questions fully and correctly.
2. Please mail copies of all documents that may relate to your complaint claim (contracts, advertisements, correspondence, proof of payment, etc.).
3. Return the information to the Consumer Protection Division (address above).
4. You may also file a complaint online. Be sure to include copies of all relevant documents.
5. PLEASE NOTE: Important "Open Records" information on page 2 of this form.

YOUR NAME AND ADDRESS:		NAME OF BUSINESS OR PERSON COMPLAINT IS AGAINST:
□ Mr. □ Mrs. □ Ms.	Age:	Name:
Name:		Address:
Address:		City, State, Zip Code:
City, State, Zip Code:		Primary Phone Number:
Primary Phone Number:		Email Address:
Email Address:		Website:

Please check appropriate box if you or your spouse are an active or former duty service member or U.S. military veteran:

□ I am an active duty service member □ My spouse is an active duty service member
□ I am a U.S. Veteran □ My spouse is a U.S. Veteran

For MOTOR VEHICLE COMPLAINTS, please list your Vehicle Identification Number (VIN):

Product or service involved:	Amount of purchase or contract:
Date of purchase or contract:	Amount paid:
Product new or used?	Form of payment (check, credit card, etc.):

Have you contacted the business or person? □ Yes □ No		Have you contacted an attorney? □ Yes □ No	
Name:	Date Contacted:	Name:	Date Contacted:

What do you think should be done to resolve your complaint fairly?

SUMMARY OF YOUR COMPLAINT – Please print or type. Use additional paper if necessary.

I understand that the Attorney General's Office is not my private attorney but represents the State of Iowa in enforcing laws designed to protect consumers from misleading or unlawful business practices. I also understand I may contact a private attorney for legal advice.

Signature_____ **Date**_____

Note: Complaints are Open Records
Under Iowa law, complaint forms or letters generally are "open records". The public has the right to review or obtain copies of open records. Also, copies of complaints are routinely sent to the person or business the complaint is directed against.

Please contact the Consumer Protection Division if you have questions about the "open records" law.