









NC Attorney General Roy Cooper

STAY SMART AND STAY SAFE!



State of North Carolina

Department of Justice P.O. Box 629 Raleigh, North Carolina 27603

We all need to keep up our guard against crooks and con artists. This booklet lists many of the scamming techniques being used against North Carolinians. Please use it to educate yourself and your loved ones about these threats to financial security and peace of mind.

This edition adds five new scams, and information to help consumers avoid being victimized by crooks. In two of the new scams, found on page 5, con artists pose as Federal agents. Crooks masquerade as computer technical support experts in a new scam found on page 7. In the other two new entries, on pages 15 and 18, shady businesses exploit consumers who want to tap into their pensions or cut their home energy costs. Finally, a new section titled "Prevention" beginning on page 22 collects tips for avoiding scams, and shines a spotlight on some of the tools and tactics scammers use to commit their crimes.

While most of the scams and frauds in this booklet can be used against consumers of any age, many of them target **seniors**. Criminals try to take advantage of seniors' trusting nature, sometimes faltering memory, or financial status. Seniors are hit by scammers harder, and more often, than other consumers.

Regardless of our age, we can fall prey to cons and scams. Here are some basic rules that can help protect all consumers:

- **Guard your numbers**. Never give your Social Security number, credit card or bank account number to anyone you don't know who contacts you.
- Don't pay money up front to get a loan, collect a prize, or for debt settlement, credit repair or foreclosure help. It's illegal to require such a payment. (And if someone says you've won a lottery or sweepstakes that you don't recall entering, they're trying to scam you!)
- Say no to high-pressure sales pitches. If the offer is only good today, walk away.
- Be cautious when responding to telemarketers, door-to-door sellers, and email or text pitches. Instead of responding to unsolicited offers, decide when and where you want to go shopping.
- Avoid get-rich-quick schemes. Beware of offers that sound too good to be true, or promise huge rewards with little or no risk.

To get more consumer tips, find out about the latest scams, or report a potential scam, visit our website at www.ncdoj.gov or call us toll-free in North Carolina at 1-877-5-NO-SCAM. You can also sign up online to get email alerts from us on fraud and other public safety issues or follow us on Facebook or Twitter.

Attorney General Roy Cooper

TABLE OF CONTENTS

PART 1 – TELEPHONE FRAUD

Surprise Prize Check Scam	1
Counterfeit Checks from Phony Lottery and Sweepstakes Companies	1
International Lotteries	1
California Sweepstakes	1
Grandma / Grandpa, It's Me!	2
Credit Card or Identity Theft Insurance	2
Guaranteed Government Grants	2
Recovered Assets	2
Medicare Discount Drug Cards	3
Public Health Department – Health Care Voucher Calls	3
Phony Bank Security Officer	3
Collect Call from the Prize Patrol!	3
Phony Government Official	4
British Bond Scam	4
Montreal Barrister / Canadian Lottery Scam	4
Terrorism and Money Laundering Fees	4
Phony Customs Officer	5
Phony IRS Agent – Sweepstakes Winnings	5
Phony IRS or Treasury Agent – Overdue Taxes	5
Phony IRS Agent – Tax Refund	5
Your Telephone / Power / Gas Service Will Be Disconnected	5
Go Back To Western Union / Moneygram	6
Funds Recovery Scam	6
Wal-Mart Store Voucher Scam	6
Phony Debt Collector	6
Death Threats	7
Phony Timeshare Reseller	7
Tech Support Scams	7

Identity Theft	8
Sweepstakes Mailings – You May Already Be a Winner!!	8
Check Processing and Check Overpayment Scams	9
Overseas Money Transfers ("Nigerian Scams")	9
Your Distant Relative Has Died In Our Country	9
Health-Related Frauds and Scams	9
Medical Insurance "Gap" Policies	10
Free Prescription Meds	10
Secret Shopper Scam	10
Distraction Thefts	10
Phony Police Detectives	10
Woman in Distress at the Front Door	11
Sweetheart Scams (Face-to-Face)	11
Sweetheart Scams (Internet and Telephone)	11
Clergyman Scams and Other Scams of Opportunity	11
Promissory Note Scams	12
Utility Company Cut-Off Scam	12
Work-At-Home Scams	12
Buy an Online Store	12
Payment Processor or "Money Mule" Scam	13
Timber Harvesting Scam	13
Alarming Message from the Bank (Phishing and Vishing Scams)	13
PART 3 – PREDATORY LENDING PRACTICES	
	1 /
Predatory Mortgage Lending	
Payday Loans	14 15
PEUSION AGVANCE ACAINS	1.7

PART 4 – OTHER TROUBLESOME OR DECEPTIVE BUSINESS PRACTICES
Unauthorized Credit Card Charges and Add-ons
Certified Senior Financial Advisor and Other Impressive Titles16
Annuity Sales and Estate Planning Seminars16
Professional Charitable Solicitors
Sound-Alike Charities and Law Enforcement Groups
Phony Charity Pleas
Timeshares, Campgrounds and Land Development Schemes
Expiring Auto Warranties
Security System Upgrades
Home Energy Savings / Radiant Barriers
PART 5 – DOOR-TO-DOOR HOME REPAIR FRAUD
Falling Chimney
My Leg Went Through Your Roof, Sir!
Mealworm Scam
Attic Bracing Scam
Toilet Bowl Scam
Floor Jack Scam
Inspector Scam
Driveway Paving Scam
You Haven't Paid Us!
Your House Does Not Meet Code
Frozen Pipes Scam
PART 6 – PREVENTION
Tips for Avoiding Scams
How They Do It – Prepaid Debit Cards24
How They Do It – Caller ID
How They Do It – Fear & Excitement
REQUEST A PRESENTATION

Surprise Prize Check Scam

Unannounced and via overnight courier, you receive a check for \$500,000 drawn on the account of a major corporation. It comes with a cover letter stating that you have won a major prize in an overseas contest. The letter says you should deposit the check immediately. Your bank may initially indicate that the check appears to be drawn on a valid account. Later that day, you receive a call from the scammers informing you that taxes were not deducted from the check, and a stop payment order will have to be placed unless \$10,000 to \$30,000 is wired immediately. Days after you wire the money out of the country, your bank informs you that the prize check was counterfeit.

Counterfeit Checks from Phony Lottery & Sweepstakes Companies

You receive a check for \$2,000 to \$5,000 that appears to be from an International Lottery. Then you receive a phone call from overseas saying that you have won a million dollar lottery or sweepstakes prize in Canada, Australia or some other country. The scammer tells you that the check was sent to cover fees, taxes or insurance on the award. You are instructed to deposit the check and then wire the money to pay those fees. Ultimately your bank determines that the check is counterfeit, but you have already wired money to the overseas scammers—money that came out of your own funds.

A common variation of this scam involves a counterfeit check and a cover letter announcing that you have won an award. The letter provides a toll-free number and invites you to call for further instructions. When you call, the scam proceeds as described above: you are instructed to deposit the check and then wire the money to cover fees, insurance and taxes on the award. But the check is counterfeit and the scammer keeps the money that you send. *For more on check scams, see page 9.*

International Lotteries

A caller offers to enroll you in the best overseas lottery opportunity each week. As a convenience to you, the caller proposes to charge the cost of this service to your credit card or checking account. You are typically charged \$10 to \$100 a week for months. Occasionally, the scammer may offer a special opportunity on a sure bet lottery package for \$5,000 – \$10,000. The scammer will pay out small sums in "winnings" from time to time to keep you interested, but the scammer is not really enrolling you in any lotteries.

California Sweepstakes*

A caller says that you have won a sweepstakes in California and requests your bank account numbers to ensure payment of California taxes on the award before you can receive it. Your bank account is debited \$200 to \$400 the following day. Unauthorized debits may occur several more times during the following weeks.

"Grandma / Grandpa, It's Me!"*

A young caller begins their conversation, "Grandma (or Grandpa), it's me! Don't you know who this is?" If you volunteer the name of a grandchild, the caller adopts that name and then pretends to need assistance. The caller begs "please don't tell my parents" because they say they've been arrested, hospitalized, had a car wreck or gotten in trouble. They sometimes use information about your family from Facebook or other online sources to help convince you that the call is legitimate. The fake grandchild then sends a friend to your home to pick up cash or a check or asks you to wire them money. Losses can range from \$200 to \$20,000. If you wire money, another scammer may call pretending to be an attorney or a jailer requesting more money for bail or fines. They may pretend to be beating or abusing the child during the call. To confirm your real grandchild's safety and stop the scam in it tracks, call their cellphone even if you've been told that it was confiscated or lost.

Credit Card or Identity Theft Insurance

A caller claims to be able to protect you from identity theft and from thieves who might steal your credit card numbers using the Internet. The caller warns that thieves will run up hundreds of thousands of dollars in debts in your name, and that you will be liable unless you purchase protection for \$200-\$600. In fact, federal law already protects you from liability for such theft and for misuse of your credit card numbers.

Guaranteed Government Grants

A caller says you appear to be qualified for a free, guaranteed government grant because of your age, employment status, or where you live. The caller asks a few questions, such as, "Have you ever been delinquent on your taxes or been convicted of a felony?" When you say "no" the caller says you definitely will receive the grant. The caller then requests your bank account information in order to deposit the grant money. But instead of putting money in, the scammer withdraws money and you don't receive any grants. Victims often lose several hundred dollars. Another version of this scam lures you into paying thousands of dollars for help applying for grants.

Recovered Assets

You receive a postcard informing you that money or property belonging to you has been located. The postcard urges you to call a toll-free number for further details. When you call, you are asked to provide financial information including your checking account number, Social Security number, and your mother's maiden name in order to have the money or property released. If you provide the information your checking account will be electronically debited, sometimes repeatedly, and you may also become a victim of identity theft.

Medicare Discount Drug Cards*

A caller offers you a Medicare drug discount card with tremendous benefits. You are asked to give your banking account numbers so your account can be debited to pay for the discount card. But you receive a card that is not honored by pharmacies in your community, or you receive nothing at all. Meanwhile, the scammer withdraws funds from your checking account for items or services you didn't order.

Public Health Department – Health Care Voucher Calls

You receive a call from someone who says they are a state or local public health official. These callers, who are often persistent and aggressive, claim that they can provide you with special health care vouchers. They request your Social Security number and personal financial information including bank account numbers, and then debit your bank account. If you refuse to provide your information, you may be subjected to abusive comments and repeated calls. This scam usually targets low-income citizens.

Phony Bank Security Officer

Follow-up to the two preceding scams: You receive a call from someone who claims to be with your bank. The caller, a partner of the original scammer, mentions the fraudulent charges previously made against your account. After discussing the charges for a few minutes to establish their credibility, the caller requests your bank account number "in order to return the improperly debited funds." The caller then tape records you reciting your account number, and uses the tape to make additional electronic debits, usually \$200 – \$400.

"Collect Call from the Prize Patrol!" - Louis Whitehead, Sweepstakes Official

A well-spoken fraud artist calls you, claiming to represent the company whose sweepstakes commercials are currently airing on TV. He says that you have won but the "prize patrol" will drive past your house and award the prize to someone else unless you send funds (usually \$600 to \$6,000) to cover taxes on the prize. He uses the name Louis Whitehead, and calls are made from pay phones in or near the Atlanta Airport. Calls from Mr. Whitehead often begin, "Collect Call from the Prize Patrol . . . "

Phony Government Official

A caller claiming to be with the Federal Trade Commission says you have won millions of dollars in a major international sweepstakes. You must wire \$2,000 or more to a Lloyd's of London office overseas to insure the award.

Callers may also claim to be with the Social Security Administration. These scammers report that there is a problem with your Social Security records, or claim that you are entitled to additional Medicare benefits. They will ask for your personal banking information, with the goal of withdrawing funds from your account.

Other callers claim to be voter registration officials. These phony officials warn that your voter registration records are not in order and need to be corrected prior to the next election. Using this pretext, they ask for your personal information including your Social Security number.

British Bond Scam

A caller says that you have won a life-interest in a bond issued by a British bank. Monthly income generated by the bond will come to \$2,000 to \$3,000, and the bond will be registered in Canada so that it cannot be taxed in the US. You must wire \$2,500 to have it registered in your name.

Montreal Barrister / Canadian Lottery Scam

You receive a call from someone who claims to be an official with the Canadian Lottery, or a barrister (attorney) representing the lottery. He says that you have won second place prize in a large sweepstakes, \$300,000 to \$500,000, and that you must forward \$30,000 to cover Canadian taxes before the prize can be released from the company's escrow or attorney trust account. If you pay you will get a second call informing you that you have actually won first place and need to send even more money.

Terrorism and Money Laundering Fees

Victims of scams who have sent money overseas to collect a prize often receive a follow-up call from a different scammer. The caller pretends to be an FBI, IRS, or Department of Homeland Security agent. They say that your entire prize award has been impounded and will be forfeited to the US Treasury unless the funds are traced and audited to ensure that they do not involve organized crime or terrorism. To collect your prize, you must pay for the trace and audit by wiring several thousand dollars.

Phony Customs Officer

A caller claims your sweepstakes prize is in his customs warehouse. You must wire \$10,000 to \$30,000 to a "bonded customs agent" to cover customs duties before your prize can be released.

Phony IRS Agent – Sweepstakes Winnings

Follow-up to the preceding scam: After you send your payment to the phony customs agent, you receive a call from someone who claims to be an IRS agent in a nearby city. The caller says US income taxes are owed on your sweepstakes prize and it will be returned if the taxes aren't paid. Caller ID information may indicate that they are calling from the IRS, but the scammers are actually calling from overseas using Voice Over Internet Protocol (VOIP) calling technologies which can be used to fake the Caller ID number. They instruct you to send several thousand dollars to pay the taxes.

Phony IRS or Treasury Agent - Overdue Taxes

You receive a call from someone who claims to be an IRS or US Treasury agent. It can be a computer-generated recording, or a live caller who is very intimidating and may have a foreign accent. In either case, the caller says you owe back taxes and threatens that you will be arrested unless you pay up immediately. You are instructed to obtain a prepaid debit card, "load" it with funds to pay your back taxes, and call back to provide the account number on the card. In some instances a different scammer will also call, saying he is with a local law enforcement agency that is prepared to arrest you if you don't pay.

Phony IRS Agent - Tax Refund

In this version of the IRS agent scam, the fake agent is pleasant and genial instead of being aggressive and threatening. He is calling with the happy news that you are due for a large tax refund. Instead of trying to get you to send money, this time the crook is hoping to trick you into surrendering your bank account and/or social security numbers.

"Your Telephone / Power / Gas Service Will Be Disconnected"

You receive a call from someone who claims to be a representative of a utility company, and Caller ID may even indicate that the call is coming from the company. The caller says that your payments are past due and that your service will be disconnected if you don't pay immediately. You are instructed to obtain a prepaid debit card, "load" it with funds to pay your overdue utility bill, and call back to provide the account number on the card. The scammers use that information to drain all funds from the card. In some variations on this scam, the scammer asks for your bank account number or credit card number to pay the allegedly overdue bills, and makes withdrawals from your account. Phony calls threatening cutoff of utilities are usually timed for the arrival of winter or summer weather, when customers are most concerned about staying warm or cool.

Go Back to Western Union / MoneyGram

Follow-up to many of the scams listed previously: A caller will claim that the payment you recently made (for a phony utility bill, etc.) was never received. The caller will say "Send your payment again. The company will issue a refund for the first attempt when you show them the letter I am sending to you." Another variation involves a follow-up call in which the scammer, who received your money the day before, claims, "The prize you paid taxes on yesterday was a second place prize, but we now realize that you came in first place! Please send us a second wire payment in the same amount as yesterday to cover the taxes on the first place award, which is much larger."

Funds Recovery Scam

Follow-up to many of the scams listed previously: A caller says your earlier payments and winnings have been seized from a crooked sweepstakes company pursuant to a court order. The caller claims to be an attorney or court-appointed receiver. He says you can still receive your winnings if you pay taxes again, and/or his attorney's retainer fee, usually \$10,000 - \$30,000.

Wal-Mart Store Voucher Scam

You receive a call from someone claiming to represent Wal-Mart or some other major retailer. The caller says you have been selected to receive special store vouchers worth \$495 as part of a nationwide promotion, and requests a bank account number so \$4.95 can be withdrawn from your checking account to cover the costs of delivering the voucher. If you provide the number, your checking account will be electronically debited in the amount of \$495, sometimes more than once. You never receive a youcher.

Phony Debt Collector

A caller claims that you owe a large debt and threatens to file embarrassing lawsuits against you or prosecute you criminally. The phony debt collector, who may claim to be a law enforcement officer, a government official or an attorney, may threaten to come to your home or place of employment or have you arrested. He may even turn abusive and threaten you with physical harm.

In some instances the phony debt collector will claim that you owe money for a payday loan made over the Internet. You may get such a call if you have ever borrowed and repaid an Internet payday loan in the past, but you can also receive a call even if you have never applied for a payday loan online. Regardless of the approach they take, the goal of the phony debt collector is always the same: to harass you until you pay the amount demanded. *For more on payday loans, see page 14*.

Death Threats*

Follow-up to many of the scams listed previously: After you've been scammed, a caller demands more money. If you refuse, the scammer may call back and threaten to kill you, or harm you or one of your loved ones. The caller is usually based overseas and has no intention or ability to physically harm you.

Phony Timeshare Reseller

You receive a call from someone who claims to have a buyer for your timeshare property. The caller may even guarantee that the sale will go through. After obtaining authorization to debit your credit card or bank account for hundreds or perhaps thousands of dollars, the scammers sends a contract. But the fine print says the timeshare will merely be advertised for sale. *For more on timeshares, see page 17*.

Tech Support Scams

You receive a telephone call or an email from someone who claims to be a technical support expert with Microsoft or another major tech company. You are told that if you will allow them to access your computer via the Internet for just a few minutes, they can diagnose why it is running slower than it used to and take steps to increase its speed and security. For a fee, of course. If you are lucky, they just take your money and do no harm to your computer. If you are unlucky, in addition to taking your money they harvest personal, confidential information from your computer. They may also install a program that allows them to spy on you from now on. Some scammers will also lock your computer and force you to pay a large ransom to get your data back and your machine working again.

Identity Theft

You learn that someone has made purchases using your credit card, or has been issued new credit in your name. You discover that a thief masquerading as you has sold your home or vehicle and pocketed the money. You find out that someone has used your health care benefits and then stuck you with their bills.

Identity theft is the fastest growing scam in the US and has been the leading consumer complaint to the Federal Trade Commission for the past several years. Many of the scams and frauds listed in this document are designed to acquire your credit and checking account numbers, to make it easier to commit identity theft. Identity thieves especially target seniors because they often have substantial savings and little debt.

To protect against identity theft, always check your bills and account statements carefully for unusual charges and activities. Contact your bank or creditor immediately if you notice anything suspicious. Check your credit report annually by visiting www.annualcreditreport.com. Each of the three national credit reporting services must provide you with a free copy of your credit report once per year upon request. You should also consider freezing your credit.

Victims should contact the North Carolina Attorney General's Office (1-877-566-7226) or the Federal Trade Commission (1-877-ID THEFT) for an Identity Theft Victim Kit, and file a police report with a local law enforcement agency. For more information about identity theft and credit freezes, visit www.ncdoj.gov.

Sweepstakes Mailings – "You May Already Be a Winner!"*

You receive mailings from sweepstakes companies that lead you to believe that you must purchase their products in order to qualify for a prize. The mailing may also imply that you have a greater chance of winning if you buy more products. As a result you spend thousands of dollars, repeatedly purchasing the same products or magazine subscriptions, in hopes of winning the multi-million dollar prize. By law, sweepstakes cannot require you to make a purchase in order to enter, and making a purchase does not increase your chances of winning.

Sweepstakes companies have earned a reputation for being misleading, and for creating false impressions about the need to purchase their products. They reinforce these false impressions with skillfully worded mailings and expensive TV ad campaigns showing happy winners. Some companies have even been accused of identifying and targeting specific vulnerable individuals. The companies give these individuals the impression that the contest is down to them and only a few other contestants, in order to get them to make even more purchases. Again, making a purchase does not increase your odds of winning.

Check Processing and Check Overpayment Scams

You receive a letter, telephone call, or email from someone who claims that they have received a check for several thousand dollars that they cannot cash in their own country. In this variation of the overseas money transfer scam and the sweepstakes scam, the scammer asks for your help cashing the check. The scammer endorses the check and sends it to you, asking you to deposit it and keep 20 percent while sending them the other 80 percent. The check appears to be from a US car dealership, computer company or some other legitimate business, and it bears a valid account number for that business. Days after your money is wired overseas, your bank reports that the check is counterfeit and will not be honored.

Overseas Money Transfers ("Nigerian Scams")

Via fax, email, or regular mail, you receive an impassioned plea from someone who claims to live in Nigeria or another developing country. They may present themselves as a former high government official, or perhaps a relative of a former dictator. They claim to need to transfer several million dollars into the US and offer to pay you a 25 percent commission to use your account to make the transfer. The person requests absolute secrecy, and suggests the funds may not have been obtained legitimately. They may also ask for several thousand dollars, supposedly to bribe a foreign government official who is blocking transfer of the millions into your account. In recent variations of this old scam, the fax, email or letter will claim that the smuggled money is intended for orphans or a religious ministry. These are ploys to acquire your bank account number and then drain the account of funds.

"Your Distant Relative Has Died In Our Country"

In this variation of the overseas money transfer scam, you receive a message from someone who claims that you are the sole heir of a distant relative who died in a foreign country and left an estate worth millions of dollars. The estate needs to be wrapped up quickly or it will be forfeited to the government. You are asked to wire funds to help pay for some aspect of the transaction (taxes, insurance, estate administration costs, money to bribe crooked officials, etc.). After each payment the scammer comes up with another reason for you to send more money.

Health-Related Frauds and Scams*

You learn of a product or service that claims to provide relief for your illness or chronic medical condition. It comes with a money-back guarantee, which helps convince you to try it. But the guarantee usually requires you to try the product or service for at least four months, and by then the company that sold it to you has disappeared. You can some-times get a refund through your credit card company when you are dissatisfied with a purchase, but most credit card companies will not grant a refund after four months.

Medical Insurance "Gap" Policies*

You are already well-served by a combination of Medicare, Medicaid, retirement health plans or other insurance, but you are convinced to enroll in an additional health insurance plan that supposedly covers only items and charges not covered by the other policies. This costly "gap" insurance comes with several limitations, deductibles, and exclusions which makes it of little value to you.

Free Prescription Meds*

You receive letters or other messages claiming you can obtain "all your prescription medicines for free, guaranteed!" After paying a fee you receive application forms for pharmaceutical companies' free prescription drug assistance programs. You could have gotten the forms directly from the companies at no cost, and admission into their drug assistance programs is not guaranteed.

Secret Shopper Scam

You are invited to become a "secret shopper," someone who gets paid for conducting business with a company and then evaluating its performance. You receive detailed instructions on how to test the Western Union or MoneyGram wire transfer system, along with a check for several thousand dollars. You are told to deposit the check into your account, wire 90 percent of the funds to a person located overseas, and then immediately fill out an online questionnaire about your experience. Days after you deposit the check and wire the funds overseas, your bank says that the check was counterfeit and that your account has been debited in the amount of the check.

Distraction Thefts*

Thieves knock on your door, pretending to be government officials or utility company employees. They claim to be providing low-cost home renovation or energy savings projects, and they ask to enter so they can take measurements. While measuring rooms and windows they pocket valuable items or look around for larger valuables, such as antique furniture, that can be stolen while you are away. These thieves often work in pairs. One will occupy you while their partner steals items in other rooms.

Phony Police Detectives*

In this variation on the distraction theft technique, scammers knock on your door claiming to be plainclothes police detectives. They are on the hunt for criminals or escaped prisoners, and they say the escapee mentioned your name and address to others who are now in custody. They ask permission to look around the house or apartment. While one of the phony detectives distracts you, the other steals valuables.

Woman in Distress at the Front Door*

In this variation on the distraction theft technique, two women knock on your door. One says that the other is pregnant and in distress, or needs assistance of some kind. They ask to come inside and use the telephone. While one is on the telephone pretending to call for help, the other, who is feigning distress, asks to use your bathroom. Instead, she steals money, credit cards, jewelry and other small valuables. The women are members of a roving fraud group. After the telephone call, a male member of the group shows up at the curb and drives them away.

Sweetheart Scams (Face-to-Face)*

You are befriended by someone who eventually pretends to be in love with you. If you are an elderly widow or widower, you may be targeted because you are believed to be lonely. His or her short-term goal is to secure gifts and loans, but the ultimate goal is to secure control of your estate or financial affairs. The "sweetheart" may accomplish this by convincing you to grant them power of attorney, or make them the primary beneficiary of your will. This scam is often perpetrated by a member of a traveling fraud group.

Sweetheart Scams (Internet and Telephone)*

You are contacted by someone (often from overseas) who has seen the personal information you posted on a social networking or dating website. The "sweetheart" uses email and phone conversations to strike up a friendship which eventually blooms into a romance. Once you are sufficiently smitten, your new love interest pretends to be in the hospital or in jail overseas and asks you to wire money to them, often repeatedly.

Clergyman Scams and Other Scams of Opportunity*

A member of the clergy exploits your religious belief and their position in order to gain control over your finances. Other symbols of authority including law enforcement officers have also been known to misuse their positions of trust. Often these individuals will try to get you to grant them a general power of attorney. Con artists look for signs of vulnerability and then prey on it. In one instance, a tree service man with no financial training gained control of a North Carolina woman's property by convincing her that he could manage it profitably.

Promissory Note Scams

You receive an invitation to attend an investment seminar at a local restaurant or hotel. At the seminar, you are sold promissory notes as an investment. The notes are issued by obscure companies and claim to offer interest rates much higher than the returns on bonds or other investments. The notes and the interest payments are said to be secured by an insurance policy. But the notes may be for a failing company, and the insurance policy may be worthless as an investment.

Utility Company Cut-off Scam*

You are contacted by an individual who presents himself as a utility company employee. The phony utility agent claims that your water, gas or electric bill is past due and that your service is about to be cut off. You can prevent disconnection by paying your bill and late charges. If the scammer is standing at your front door, he will accept cash or a check. If he has called you on the telephone, you can pay by providing your checking account or credit card number.

Work-At-Home Scams

While struggling to make ends meet, you see road signs, ads, or mailings about working at home. Lured by promises of large earnings, you agree to pay several hundred dollars for materials. The work may be stuffing envelopes with mailings inviting others to make money at home, or it might involve painting or assembling simple items and then returning them for approval and payment. These schemes seldom earn you much, if any, money.

Buy an Online Store

While searching the Internet for information about how to operate a business from your home, you get messages offering to help you establish a virtual store or e-commerce business using your home computer. The offers claim that they will create a unique website to help you sell merchandise. The merchandise you sell will be shipped directly to your customers from a third party. All you have to do is check the website from time to time, collect thousands of dollars in payments from your customers, and forward their orders via email to the third party shippers. You can get the website and all the assistance you need for two or three thousand dollars.

Most consumers who pay the fee find that selling items online is harder than they'd thought and that their earnings aren't what they expected. Once you pay the initial fee, you're also likely to be hit up for additional fees to pay for services such as accounting, management coaching, legal representation and website upgrades. You may even find charges for these services appear on your credit card or debit card without your approval. Some consumers have found as much as \$40,000 in unexpected fees charged to their accounts in a matter of weeks.

Payment Processor or Money Mule Scam

You are invited to earn money by providing international payment processing services. If you sign up, you will start to receive cash, checks and wire transfers from across the United States. Your job will be to forward the funds overseas immediately via wire transfers, after deducting a 10 percent commission for yourself. In reality, the money you receive comes from elderly fraud victims and you will be wiring it to the scammers who defrauded those victims. In many cases this scam, which makes the victim an accessory to fraud, is targeted at individuals who have themselves lost a lot of money to these same overseas scammers.

Timber Harvesting Scam*

You are approached by loggers who claim they will pay top dollar to harvest timber on your land. They promise to leave the land cleared of debris and brush, but after cutting and removing the best timber they disappear without paying. Debris and brush from the operation is left behind and the landscape has been damaged by timber harvesting equipment. In a variation on this scam, the unscrupulous loggers deduct the supposed costs of clearing debris and re-grading the soil, leaving you with a check for only a few hundred dollars.

Alarming Message from the Bank (Phishing and Vishing Scams)

You receive an email that appears to be from your bank. Because of a problem with the bank's computer or security system, the email says, you need to provide important account information immediately. The email may contain a link to a web page where the account information can be entered. But the web page, which may appear legitimate, is phony. The information you provided is used to steal money from your account.

This is called a phishing scam because crooks use bait (a message that appears to come from a trusted source) to lure you into providing confidential information. Phishing scammers pose as banks or other financial institutions, insurance companies, social networking sites, online payment vendors, online auction websites, or even the Internal Revenue Service.

Another variation of this scam, called vishing (voice phishing) starts with an email or text message that asks you to call a telephone number to provide your account information. The scammers set up an automated call menu where you enter your personal bank account numbers and other financial information using your telephone.

PART 3 – PREDATORY LENDING PRACTICES

Predatory Mortgage Lending*

An unscrupulous mortgage lender offers you a loan to consolidate your debts, help your grandchildren go to college, or pay for home improvements. But the loan is a bad deal for you because it includes a high interest rate, expensive fees for unnecessary options like credit life insurance or disability insurance, brokerage commissions, "points" and origination costs.

Your loan terms may also include a balloon payment so that the entire amount of the mortgage loan is due after just a few years. At that point the lender may offer to refinance the loan, claiming this will lower payments. Instead, more fees get tacked on to the loan.

The end result is that you can quickly lose most of the equity in your home (a process known as equity stripping) while continuing to face high payments for what might have originally been a modest mortgage loan. Predatory mortgage loans often target seniors whose home mortgages have already been paid off.

Payday Loans

Finding yourself short on cash after a car repair, medical bill, or some other unexpected expense, you apply for a small, short-term cash loan called a payday loan. To receive the loan, you write the lender a personal check. Your check is held, and then cashed on your next payday. In lieu of a personal check, some payday lenders will offer to transfer money to and from your bank account electronically.

Payday loans (also called cash advances) may seem like a quick solution to your cash crunch, but they can trap you in a cycle of debt and cost you a lot more in the long run. The loan is due in full as soon as you receive your next paycheck, typically in two weeks.

If you are like most payday loan borrowers, you aren't able to repay the loan that quickly. Instead, you get stuck taking out one loan after another without ever being able to pay them off. A payday loan of \$100 – \$500 can carry an annual interest rate of up to 680 percent. Payday lending through storefront locations has been shut down in North Carolina, but some overseas and tribal lenders continue to make payday loans online.

Consumers who apply for payday loans online are sometimes victimized by criminals. In some cases the consumer's confidential financial information, including their bank account information, is sold to the thieves. In other instances scammers operate their own fake payday loan websites, and use private information taken directly from the consumer's loan application to steal money from their accounts. For more information online payday loans, see Phony Debt Collector on page 6.

PART 3 – PREDATORY LENDING PRACTICES

Pension Advance Scams

A company offers to help you take control of your military, government or corporate pension. They promise you a fast, lump-sum cash payment. They do not tell you that you are raiding your pension and signing over the rights to it, sometimes for years. These companies disguise high-interest rate loans as pension advances, with fees and interest rates often exceeding 100 percent of the amount borrowed. In some cases the pensioner's spouse has to sign away their right to receive any pension payments until the loan has been repaid, a period that can be as long as eight years. These companies prey on people who are having financial difficulties.

PART 4 - TROUBLESOME / DECEPTIVE BUSINESS PRACTICES

Unauthorized Credit Card Charges and Add-Ons

After a recent credit card purchase in person or over the phone, you discover additional charges on your account. The charges could be for a credit card protection plan, a discount buying service, or a travel program. They have been placed on your account without authorization, although in some instances the merchant or telemarketer may have briefly mentioned the extra service or product. However, the charges are added without getting your clear consent. You should always dispute these charges promptly with your credit card company and the merchant.

"Certified Senior Financial Advisor" and Other Impressive Titles*

Some salespeople have official-sounding titles to give you the impression that they have been approved by a governing body or organization. Sellers of annuities, estate planning services and other products and services often adopt titles such as "Licensed Senior Financial Consultant" or "Certified Estate Planning Advisor" in order to appear more legitimate. The supposed licensing or certifying agencies often do not exist, or they are controlled by the marketers themselves.

Annuity Sales and Estate Planning Seminars*

You are invited to an estate planning seminar. While many estate planning seminars are legitimate, others are not. Deceptive seminars often hide behind names that make them sound like non-profit organizations for seniors. In reality, the people conducting the seminar want to sell you a living trust estate planning package as well as unneeded insurance policies, annuities, or investments. You may end up paying more for this living trust plan than you would if you went to an estate planning attorney for advice. Additionally, their plan for your estate may result in huge commissions for them and expensive problems for you or your heirs in the future. Scare tactics are often used to encourage seniors to liquidate their holdings and invest in long-term deferred annuities, which are generally not appropriate investments for people over 75 years of age.

Professional Charitable Solicitors

You are contacted by a professional fundraiser on behalf of a legitimate charity or community group. Unless you ask, fundraisers do not have to tell you how much of your donation they will keep. Some keep as much as 90%, so ask how much of your contribution would go to the worthy cause and how much would go toward fundraising. You can also ask to receive written information about the charity's fundraising. Instead of responding to individual solicitations, you may want to contribute directly to your favorite legitimate charities.

PART 4 - TROUBLESOME / DECEPTIVE BUSINESS PRACTICES

Sound-Alike Charities and Law Enforcement Groups

Some questionable charities try to deceive you by using names that are similar to well-known, legitimate charities. They often adopt names that sound like law enforcement agencies because they know people generally support law enforcement, and because some people may be intimidated by a call from someone who claims to be with a police organization. Ask the caller to send you information by mail so you can check out the organization before contributing to them. If you want to support a particular group, such as your local police or schools, contact them directly to find out the best way to do so.

Phony Charity Pleas

Some scammers use recent events, such as natural disasters and other tragedies, to try to trick you into giving them your money. Don't respond to unsolicited emails and text messages asking you to give. Even if the messages look legitimate, they could be fraudulent. Also, be careful of social networking posts asking you to donate. The cause may sound worthy, but you have no way of verifying how your money would really be used. If you want to help a particular cause or give to victims of a disaster, contact an established charity rather than responding to questionable solicitations.

Timeshares, Campgrounds and Land Development Schemes*

Marketers often use high-pressure tactics to convince you that purchasing their time-share, campground membership or resort property share will be a good investment. However you may find that your purchase does not gain value, is difficult to use, and leads to years of expensive maintenance and membership dues or property taxes. You may also discover that it cannot be sold easily, and that people who claim to have a buyer for your property are really just scammers out to steal your money. [See page 7.] In some cases, marketers try to convince you to pay additional money to exchange your time share or campground membership for a vacation club membership with promises that the new membership will be better for you when that may not be the case. Resist high-pressure sales tactics, and take home written materials to review rather than buying on the spot. If you intend to leave the property to your adult children, carefully review the materials with them before purchasing. Seniors are often targeted by these scams with claims that buying the product will benefit their children and grandchildren.

Expiring Auto Warranties

Four or five years after buying a car, you get a letter or call saying that your existing warranty is about to expire and should be extended. These extended warranties or service contracts, which are not offered by car manufacturers, are very costly and rarely live up to expectations. Car dealers may refuse to submit claims under the extended warranty, you often have to pay a deductible for each repair, and many repairs aren't covered at all.

PART 4 - TROUBLESOME / DECEPTIVE BUSINESS PRACTICES

Security System Upgrades

You are approached by someone who claims to be a representative of your home security system company. He says he needs to upgrade your alarm system. He examines it, makes some phone calls, and then has you sign a document agreeing to upgrade your system. Actually, he works for a different security company and he has just conned you into signing a two-year contract with them. The new company charges more than your old one did and in addition to your higher monthly cost, you may owe money to your old alarm company if you broke a valid existing contract.

Home Energy Savings/ Radiant Barriers*

You receive a call from a company offering a free survey of your home's insulation. After the survey is completed, the company representative promises significant energy savings, typically 25% or more, if you install their products. The cost is usually several thousand dollars. If you agree your home will quickly be fitted with things like energy-saving compact fluorescent light bulbs, weather stripping on your windows and doors, insulation on your water heater and pipes, and insulation in your attic and electrical outlets. But the savings are nowhere near what the company promised. Some companies also make unrealistic claims about radiant barriers, which are shiny panels or flexible membranes used in construction. Radiant barriers are designed to slow the transfer of heat. But scammers, who frequently cite use of radiant barriers by NASA in space vehicles, say installation of the barriers will lead to significant energy savings. The barriers, which often are not even installed as intended, deliver little or none of the promised savings.

.

PART 5 – DOOR-TO-DOOR HOME REPAIR FRAUD

Falling Chimney*

A contractor knocks on your door and says your chimney is separating from your house. He claims it might fall on the neighbor's house or yard, and he says he can secure it. He and his crew place a useless metal strap around the perfectly sound chimney and charge you \$800 – \$2,000 for their work.

"My Leg Went Through Your Roof, Sir!"

A man offers to clean your gutters for a small fee. Afterwards, he shows you pieces of rotten wood and claims your roof is rotting: "my leg went completely through it." He says the entire roof needs replacing and he can have a crew there in minutes to do the work. The crew comes and lays new shingles over the perfectly good roof. They demand \$7,000 - \$8,000.

Mealworm Scam*

Adding a scam on top of a scam: the same roof repair crew may show you a bag full of worms. They claim that the worms are consuming the wood in your attic, and offer to kill the pests by spraying in the attic. In fact, the critters are often mealworms commonly used to feed small pets. They spray your attic with a mixture of water, kerosene and other smelly substances. Usual charge: \$1,000 - \$3,000.

Attic Bracing Scam*

A different follow-up scam: The crew says repairs to the roof have weakened the rafters in your attic. They offer to brace them so the roof will not collapse. They hammer two-by-four studs between the rafters and the floor of the attic, and then charge \$100 for each of these "braces." The braces, often called "stiff knees," are unnecessary and can actually cause damage to the ceilings of rooms below during high wind or heavy snow.

Toilet Bowl Scam*

A member of a work crew asks permission to use your bathroom. He pours water on the floor around the base of the toilet, and then says the toilet has been leaking and might have rotted the wooden sub-floor. After inspecting the crawl space, he says that the bathroom floor is rotten and dangerous, and must be replaced. After hanging out in the crawl space and pretending to fix the floor, they charge you several thousand dollars.

.

PART 5 – DOOR-TO-DOOR HOME REPAIR FRAUD

Floor Jack Scam*

A home repair crew chief points out that your living room floor vibrates when his largest crewman walks across it. He asks to inspect the floor from below, and emerges to announce that the floor may collapse unless it is braced with heavy jacks. The crew installs several inexpensive and unnecessary metal "screw jacks" from a hardware store, and charges \$500 for each jack installed.

Inspector Scam*

After you've been scammed one or more times, the scammers may send someone to your home pretending to be the quality control inspector. The inspector claims all of the previous repairs were performed incorrectly. He says they need to be re-done before the local building inspector finds out and condemns the home. The fake quality control inspector promises to file a lawsuit against the scammers and help you recoup your lost money if you hire him to re-do the work.

Driveway Paving Scam*

A paving contractor knocks on your door. He says his crew just paved another driveway in the neighborhood. He claims to have some leftover paving material and offers an excellent deal on paving your driveway. The driveway is coated with an oily substance or a very thin layer of asphalt. Not long after you pay \$3,000 - \$6,000 for your driveway, the new surface crumbles or washes away. This scam is perpetrated by roving contractors who strike an area and move on quickly.

"You Haven't Paid Us!"*

Some of the same fraud artists who use the driveway paving scam will also sometimes confront you and angrily demand thousands of dollars for work they supposedly performed several months earlier. They may threaten lawsuits, property liens, or worse in order to get you to pay for work that they never actually performed. If the fraud artist perceives that you may have short-term memory problems, they might use a softer approach: "Sir, don't you remember telling me to come back today to get paid?"

"Your House Does Not Meet Code"*

An unscrupulous home repairman tells you that your home isn't "up to code" and recommends extensive renovations so it will not fail an inspection. In fact, older homes are not required to meet contemporary building codes, and building inspectors do not make unsolicited visits to determine if existing homes meet current standards.

PART 5 - DOOR-TO-DOOR HOME REPAIR FRAUD

Frozen Pipes Scam*

During very cold weather, a crooked home repairman claims that pipes under your home appear to be frozen. The pipes will flood and cause structural damage if they are not repaired before they thaw. The scammer pretends to repair the pipes and then collect \$1,000 or more.

TIPS FOR AVOIDING SCAMS

Telemarketing Scams

- 1. Place your home and cell phone numbers on the Do Not Call Registry at 1-888-382-1222 or www.donotcall.gov to cut down on unwanted telemarketing calls. Go online anytime to verify that your phone numbers are still registered.
- 2. Never give out important numbers like your bank account, credit card or Social Security number to anyone who calls you.
- 3. Many robocalls are illegal. If you receive a robocall, hang up. Do not press a number to avoid further calls. This alerts robocallers that they have reached an active number and could actually lead to more unwanted calls.

Sweepstakes Scams

- 1. Throw away unsolicited lottery or sweepstakes mailings that say that you are a winner. Foreign lotteries are illegal and the checks they send are fake, no matter how real they look.
- 2. Never send money to get a prize. It's illegal to require a payment before you can receive a prize. It's also against the law to charge an upfront fee to receive a credit card or get a loan.
- 3. Don't be pressured to buy something in order to enter a sweepstakes. You don't have to buy to enter, and buying doesn't increase your chances of winning.
- 4. Don't put bank account or Social Security numbers on entry forms for sweepstakes or other contests.

Investment Scams

- 1. Never agree to invest in or buy something you don't understand.
- 2. Read all forms completely, and consult with a knowledgeable friend or trusted professional, such as a lawyer or an accountant, before you sign anything.
- 3. Don't make a quick decision about investment offers or changing insurance policies. When a loved one dies, avoid making major financial decisions or purchases right away.
- 4. Beware if a salesperson says "it's a special opportunity, but you have to keep it secret," or urges you to "act now" while using phrases like "limited offer," "risk free" or "tax-free offshore investments."
- 5. Remember, all investments include some risk and you can't get something for nothing.

Health Care Scams

- 1. Avoid products that claim to be miracle cures or scientific breakthroughs, or say they contain a secret ingredient. Be skeptical of marketing that uses personal testimonials by consumers or doctors claiming "amazing results."
- 2. Products that offer a "no-risk money-back guarantee" often don't live up to that claim.
- 3. Promotions that promise a free meal or lodging usually include a high-pressure sales pitch.
- 4. Don't sign up for any discount health or drug plan before checking with your doctor, pharmacist or the Attorney General's Office.

Home Construction and Repair Scams

- 1. Be very skeptical of unsolicited offers for home repairs, especially if the contractor comes to your door and says the job needs to be done right away. Don't let them pressure or scare you into paying for a phony repair.
- 2. After a disaster of any kind, beware of scammers who come to your home posing as government officials or insurance adjusters. Contact the government agency or your insurance company to verify before you let them inside or have work done.

When you need work done on your home, ask friends or coworkers for recommendations. Get written estimates from the contractors you are considering and check on references, insurance, and license.

- a. General contractors (<u>www.nclbgc.org</u> or 919-571-4183)
- b. Electricians (<u>www.ncbeec.org</u> or 919-733-9042)
- c. Plumbers and HVAC (www.nclicensing.org or 919-875-3612)
- 3. When you select a contractor, get a written agreement that states clearly the exact costs, work to be performed and completion dates.
- 4. Don't pay before the work begins. Instead, make payments as work is completed or once the job is done. Never make a final payment until work is complete to your satisfaction.

Charity Scams

- 1. Research unfamiliar charities before you donate. Beware of fake and "sound alike" charities that try to exploit your sympathy for victims of a recent disaster.
- 2. When a charity calls, ask whether the caller is a professional fundraiser and find out how much of your contribution will go to fundraising costs.

- 3. Scam artists will pose as representatives of a charity and lie to get your money. Be wary of messages reminding you to fulfill a pledge that you don't recall making, and requests to make a second donation when you don't recall having donated before.
- 4. Do not send cash donations. Cash gifts can be lost or stolen. For security and tax record purposes, it's best to pay by credit card. If you pay by check, make it out to the charity itself, not the fundraiser.
- 5. Instead of responding to requests to donate, do your own research and decide when and to whom you want to give.

HOW THEY DO IT

Prepaid Debit Cards

Overseas and out-of-town scammers who don't deal with their victim face-to-face have always faced this challenge: "Now that I've tricked him/her into believing me, how can I take delivery of their money?" For many years, these con artists relied on electronic transfer of funds via companies like Western Union and MoneyGram. Scammers would have their victims take money to the local office and "wire" the money to them.

Now the rise of technology, coupled with changes in the banking industry, has led to the development of reloadable prepaid debit cards. These cards have legitimate uses, but they can also be used to facilitate fraud. They've become very popular with scammers.

Once a victim is on the hook, the scammer directs them to purchase a card and load it with funds. Then the victim is directed to read the card number to the scammer over the phone. The scammer counterfeits the card in Jamaica or the United Kingdom, and drains all the money from it. Crooks found prepaid debit cards that utilize a scratch-off system to be particularly useful in exploiting victims. One of the biggest prepaid card companies has pulled its scratch-off product from the market, but other companies still offer scratch-off cards.

Caller ID

Caller ID is a handy telephone feature that can indicate who is calling, but consumers can't rely on it. That's because crooks have figured out how to turn it into another trick they can use to help steal money from unsuspecting victims.

Anyone who gets their phone service through an internet provider can download special software and use Voice over Internet Protocol (VoIP) calling technologies to fake a Caller ID number. A

call that appears to be coming from a consumer's bank or utility company, a charity, or a government agency could actually be a scammer. Fake Caller ID is also used by crooks pretending to offer online tech support for home computers. Overseas scammers can even make their calls look like they originated in the United States.

Caller ID can be helpful, but smart consumers know that just as you can't judge a book by its cover, you can't judge a telephone call by its Caller ID.

Fear & Excitement

Scammers know that knocking us off-balance is the best way to get past our usual skepticism and suspicions. And they know that two of our emotions... fear, and excitement... offer the best shortcut.

Crooks use **fear** in scams like the Extended Auto Warranty scam. When your vehicle's warranty is about to expire, they send you an official-looking form offering you the opportunity to extend the warranty.

In an attempt to trick you into calling their toll-free number right away, the mailing will usually say "2nd Attempt" or "Final Notice" in a prominent spot to make you think that you misplaced the previous mailing. (There wasn't one.) If that doesn't work, they are hoping that the "Time Sensitive" stamp on the mailing (and the rapidly approaching expiration of your warranty) will scare you into calling immediately without examining the offer to see if it is worthwhile. (Most extended warranties aren't.)

Crooks use **excitement** in a variety of scams including those involving sweepstakes and lotteries. The basic idea is simple: First, convince you that you have won a large cash prize. This can often be accomplished with an official-looking check or mailing, or a convincing call from someone who claims to represent the sweepstakes or lottery.

Once you are excited about winning, your natural skepticism takes a back seat. So when you are told that you owe taxes on your prize and they must be paid before you can collect it, the scammers tell you to write a large check ("Why not? You're RICH now!") and send it off. When the dust settles and the scam is revealed you'll be on the hook for the check you wrote, while the scammers who victimized you will have cashed your check and gone on their merry way.

Now that you know some of their tricks, hopefully you'll find it easier to keep your emotions in check the next time you are exposed to a scam.

REQUEST A PRESENTATION

The North Carolina Attorney General's Office can provide presentations about scams and identity theft to groups of consumers.

For more information or to schedule a presentation for your group, please contact:

Victims and Citizens Services
North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, North Carolina 27699-9001

Telephone: 919-716-6783

Email: outreach@ncdoj.gov

Telemarketing information in this booklet (V09-13) is provided by NC Attorney General Roy Cooper's Telemarketing Fraud Prevention Project, US Department of Justice Grant # BJA 1999-LS-VX-0004, and Grant # 2003-DD-BX-0318, NC Governor's Crime Commission Grant # PROJ009450.

Thanks to Assistant Attorney General David Kirkman of the Consumer Protection Division for his ongoing work to catalogue and fight scams against seniors and other consumers.