The New FedUp Handbook
Senior Fraud Education and Protection Program
www.NJConsumerAffairs.gov 1-877-746-7850
New FedUp

Senior Fraud Education and Protection Program

Introduction
Dear New Jersey Consumer,

The New Jersey Division of Consumer Affairs is committed to empowering senior citizens and all other consumers, by providing the information and awareness necessary to protect themselves and their loved ones against fraud.

This FedUp (Senior Fraud Education and Protection Program) booklet and our FedUp seminars provide a practical toolkit for self-protection when doing business, avoiding scams, protecting your identity and credit, making investments, applying for mortgages, and managing your health. It includes standard, classic, common-sense advice. It also draws upon current consumer complaints and fraud alerts, and our agency’s own consumer protection investigations and legal actions.

The Division of Consumer Affairs is your resource for important consumer information. For information about a New Jersey business or professional license, or to report suspected fraud, call our Consumer Service Center at 800-242-5846.


Sincerely,
New Jersey Division of Consumer Affairs
# Table of Contents

## Chapter 1: **DOING BUSINESS**

- **Buying and Hiring** ................................................................. 1
- **New Jersey’s Lemon Laws, Auto Sales and Auto Repair** ........... 4
- **Home Repair** ...................................................................... 7
- **Charities** ........................................................................... 9

## Chapter 2: **AVOIDING COMMON SCAMS**

- **Phishing and Internet Safety** .................................................. 13
- **Impostor Scams** .................................................................. 16
- **Online Buying and Selling Scams** ........................................... 19
- **Sweepstakes and Telemarketing Scams** ................................. 23

## Chapter 3: **PROTECTING YOUR IDENTITY AND CREDIT**

- **Identity Theft** .................................................................. 27
- **Credit and Debt** ................................................................. 30
Table of Contents

Chapter 4: INVESTMENTS AND MORTGAGES

Investment and Securities Fraud ................................................................. 35
Mortgage Scams ..................................................................................... 40

Chapter 5: MANAGING YOUR HEALTH

Prevent Prescription Drug Abuse ............................................................ 45
Be Smart with your Medications ............................................................. 47
Choosing a Doctor .................................................................................. 51
In-Home Care .......................................................................................... 53
SHIP and AAAs ....................................................................................... 55

ADDITIONAL RESOURCES ..................................................................... 57
Chapter 1 - Doing Business
BUYING and HIRING

New Jersey’s businesses, as a whole, are honest and professional. They take pride in providing services in good faith to those who pay for them. It is in their best interest to maintain fair business practices and a trustworthy marketplace.

However, fraud does exist. New Jersey consumers lose hundreds of thousands of dollars annually to bait-and-switch tactics, refusals to provide refunds for shoddy work, and many other scams. The New Jersey Division of Consumer Affairs enforces the State’s Consumer Fraud Act and related laws and regulations. We can help if you have been scammed, but it is far better to protect yourself, and prevent fraud before it happens.

**Before making a purchase or hiring a contractor:**

Contact the Division of Consumer Affairs at 800-242-5846, or www.NJConsumerAffairs.gov, to learn whether the individual or company has been the subject of consumer complaints.

Find out whether the State requires a license or registration for the business and, if so, ask Consumer Affairs whether this operator’s license or registration is valid. If the business is licensed or registered, demand a copy of its liability insurance policy, and contact the insurer to find out if the policy is still valid.
Learn as much as possible about the company with whom you’re doing business. It’s often better to work locally, and deal with companies that list an actual street address, than to work with companies that refuse to provide clear information about where they are located. Speak with others who have used the company— and, if possible, find references other than the ones the company provides. Conduct an Internet search to learn about the company’s reputation. Look for positive or negative consumer reviews.

Be sure you know what you are purchasing. Can you see and touch the actual item you’ll be buying? Can you prove it includes every feature you’re being promised? Can you check for defects? If not, these may be signs of a scam.

Avoid high-pressure sales tactics. Are you being told you must decide now, without a chance to go home and think it over? This, too, could be the sign of a scam.

It is very important to get a written estimate for services such as car repair. Make sure the estimate includes clear information about the full cost. This should include a provision that the price won’t go up due to extra work or complications, without your consent.
Obtain a written contract and make sure you fully understand its terms. Make sure it includes the refund or return policy, warranty information, the full scope and details of the goods and services for which you’re paying, and the final price. Do not sign the contract until you’ve read all of the fine print and you agree with the conditions.

Consider paying by credit card because this means of payment provides a clear record that will enable you to dispute the charges with your credit card provider if you are cheated. Check your credit card statements each month for unexpected charges, such as “subscriptions” or “service plans” you never requested.

Keep copies of all contracts, estimates, receipts and other paperwork. This will make it easier to obtain a refund, or work with the Division of Consumer Affairs to pursue restitution, in case something goes wrong.

If you suspect you have been scammed, contact the Division of Consumer Affairs’ Consumer Service Center hotline at 800-242-5846. An investigator will seek a resolution and, if necessary, guide you through the process of filing a formal complaint.
NEW JERSEY’S LEMON LAWS, AUTO SALES and AUTO REPAIR

New Jersey consumers typically report more complaints about car sales and auto repair than about any other type of transaction. Most auto dealers and repair shops simply wish to earn an honest dollar. But when spending money on such important items as your car, motorcycle, or motor home, it is very important to protect yourself.

New Jersey’s Lemon Laws— New Jersey’s New Car Lemon Law protects consumers who purchase a new motor vehicle that develops serious defects on the parts covered by the warranty, that substantially impairs the use, value, or safety of the vehicle, and which the dealer or manufacturer cannot repair. The Used Car Lemon Law protects consumers who purchase vehicles no more than seven model years old, with mileage not in excess of 100,000, and a purchase price of at least $3,000 from a licensed dealer. The used-car law requires dealers to provide a limited warranty, and applies to vehicles with problems under the warranty. New Jersey also has a Motorized Wheelchair Lemon Law to protect consumers who rely on these mobility devices.

The Lemon Laws enable consumers to have their complaint heard before an administrative
law judge. For complete details and requirements, or to speak with a representative, contact the Division of Consumer Affairs’ Lemon Law Unit at 973-504-6226. Request a copy of a free booklet, “NJ Motor Vehicle Lemon Law: Your Road to Relief,” which is also available at www.NJConsumerAffairs.gov/RoadToRelief.

Auto Sales—You can kick the tires, open the hood, and check the body for rust, but that won’t tell you whether the car sustained serious damage and was subsequently repaired. Past damage can cause electrical or mechanical problems that surface long after the seller is gone. New Jersey’s Consumer Fraud Act and Motor Vehicle Advertising Regulations make it **unlawful to advertise a car for sale, without disclosing past damage**, or failing to disclose past rental or fleet use of a vehicle. In 2010 and 2011, the Division of Consumer Affairs obtained settlements from five used-car dealers who agreed to pay $240,000 after being accused of doing just that.

Separately, in 2009 the Division of Consumer Affairs took action against a car dealership accused of a number of dishonest practices. The dealership allegedly failed to pay off the loan balances for traded-in vehicles, leaving the original owners on the hook for their old loans. The dealer was also accused of misrepresenting the prices of vehicles in order to attract consumers, a practice known as “bait and switch.”
Before buying a used car, look for the **Used Car Buyer’s Guide**, which must be posted in plain view on the car. The Guide will describe the warranty, or state whether the car is offered without a warranty. Obtain a vehicle history report from the dealer, or get one yourself from a reputable source; this will let you know if the car has been damaged in the past. Test drive the car, listen for noises, and make sure all gauges, lights, air conditioning and electronic systems work. Look for signs of water or accident damage, or unusual tire wear which may indicate an alignment problem. Remember that it’s unlawful for the seller to misrepresent the vehicle’s mechanical condition, or fail to disclose any material defect subject to a warranty, if the dealer is aware of it. If you don’t like the deal being offered, or if you feel pressured, simply walk away.

**Auto Repair** - Following a 2010 investigation, the Division of Consumer Affairs accused an auto repair chain of charging consumers for work that was never actually performed on their cars, and with selling motor vehicle inspection services when its stores were not licensed by the Motor Vehicle Commission to perform inspections. The chain settled for $250,000 and agreed to change its business practices.

How can you be sure you’re getting an honest deal when you bring your car in for repairs? Call the Division of Consumer Affairs and ask about any past actions or consumer complaints.
against the repair shop. Get a cost estimate in writing. **Remind the mechanic to get your authorization before making repairs that are not listed on the original repair order.** If you believe the mechanic has recommended unnecessary work or you are dissatisfied with the estimate, get a second opinion. If the work is guaranteed, get all of the warranty information in writing on the repair order or bill.

**HOME REPAIR**

Know your rights before opening your home to a contractor. Home improvement contractors (HICs) are required to register with the Division of Consumer Affairs. Other occupations—electrical contractors; fire and burglar alarm installers and locksmiths; heating, ventilating, air conditioning and refrigeration (HVACR) contractors; and master plumbers—must be licensed by one of Consumer Affairs’ professional boards.

The vast majority of these contractors are honest professionals, but you should protect yourself before signing a contract. “Home improvement” is typically the second-most common consumer complaint category reported to the Division of Consumer Affairs.

When hiring an HIC or a licensed contractor, obtain his or her New Jersey registration or
license number. (Note: HICs include roofers, waterproofers, fence installers, carpenters, certain landscapers, and many others. If you’re not sure, call the Division of Consumer Affairs). Call the Division of Consumer Affairs to learn whether the registration or license has expired, and whether consumers have complained about the contractor.

**Obtain a copy of the contractor’s liability insurance policy**, and call the insurer to learn whether the policy is still valid. Speak with references who know about the contractor.

**Be wary of contractors who insist on a large up-front payment** (the customary arrangement is one-third in advance, one-third halfway through the job, and one-third upon completion); and contractors who say there is no need for a written contract (under State law, written contracts are required for projects costing $500 or more). Most important, be wary of contractors who offer unsolicited services (such as knocking on your door and saying, “We were just in the neighborhood and can give you a good deal”). This is often the first step in a scam.

**Read the contract thoroughly before signing it or paying any money.** Make sure it clearly explains the scope of the project, the time frame, the estimated final cost, and that it clearly specifies the brand names and the quality of materials that will be used. Be sure it clarifies
whether the contractor will hire sub-contractors (and who will be responsible for paying them) and be sure to learn as much about the subcontractors as you do about the contractor.

**Consider your financing options.** Shop for credit, and be sure you understand the annual percentage rate (commonly called “APR,”) you’ll have to pay. We recommend that you do not pay cash (even if the contractor tries to make cash sound attractive by saying, “You won’t be charged sales tax”), and do not pay for the entire job up-front.

**CHARITIES**

Consumers should know exactly where their gift is going, before donating to a charity. Legitimate charities will encourage you to ask questions, learn about their programs, and review their financial reports before you make a donation. Others hide behind vague but positive-sounding mission statements.

**Investigate Before You Donate.** You can obtain information about a charity in several ways. Call the organization and ask. Visit the charity’s website. You can also visit the Division of Consumer Affairs’ Charities Registration page at [www.NJConsumerAffairs.gov/ocp.charities.htm](http://www.NJConsumerAffairs.gov/ocp.charities.htm) and search for the charity by name, or call the Division’s Charities Hotline at 973-504-6215.

Find out whether the charity is registered to solicit in New Jersey, or is exempt from having to
register. Certain religious and educational organizations, and charities whose annual income comes to less than $10,000 in public contributions and fundraising, are exempt.

Learn about the charity’s stated mission and the programs that support its mission.

Find out how much the charity spent during recent fiscal years on program costs, management costs, and fundraising. According to the Better Business Bureau’s “Standards for Charity Accountability,” a charity should dedicate at least 65 percent of its expenses toward charitable programs, and no more than 35 percent on fundraising. Compare that guideline with the expenditures reported by any charity that asks you for a donation.

The Division of Consumer Affairs keeps an updated list of “New Jersey’s Top 10 Most Inquired-About Charities” at www.NJConsumerAffairs.gov/charity/inquired/#list, with pie charts that detail each organization’s expenditures.
Don’t be fooled by a charity’s convincing name, and don’t fall for a sad story. Unfortunately, many so-called charities turn out to be frauds that deceive donors, then pocket the money.

In the wake of the 2011 earthquake and nuclear disaster in Japan, one scam artist sent out e-mails falsely using the name of a respected charity that helps children in disaster zones. The con artist asked people to send donations via Western Union to an address in the Philippines— a method that is not used by the charity he was impersonating.

**Beware of high-pressure solicitations.** This includes phone calls urging you to donate immediately, or letters threatening to report you to a credit rating agency because you “promised” to make a donation. Even if you agreed over the phone that you would donate, you are not obligated to make the donation – especially if you start to get a bad feeling about the organization.

Ask whether the charity uses professional fundraisers— especially if its fundraiser is on the phone demanding a donation. **Some paid fundraisers keep as much as 80 percent of the money you donate, and give only 20 percent to the so-called charity.** New Jersey law requires paid fundraisers to identify themselves and answer your questions honestly.
Chapter 2 - avoiding common scams
PHISHING and INTERNET SAFETY

The Internet is a powerful tool that can enrich our lives— or open us up to identity theft. As with any invention, we can safely enjoy the Internet’s benefits as long as we remain alert, and take basic steps to protect ourselves.

Beware of phishing and related psychological tricks. Computer hackers use the term “social engineering” to describe methods by which they get victims to hand over their passwords, usernames, credit card information or other sensitive data without thinking twice. Once you have given up this information, you are a prime target for identity theft.

Social engineering can take the form of e-mails or instant messages that appear to come from an official or friendly source. You may get a fraudulent e-mail that appears to be from your bank, an online payment processor, a shopping website, or a social networking site. For example, the e-mail may claim your bank needs an update of your account information. The e-mail or instant message may ask you to download an attachment. Click on it, and you may be downloading a “Trojan horse” virus that lets the criminal spy on all of the information on your computer. Or … the e-mail or instant message may direct you to a fake website.
that looks almost identical to the official website of your bank, or an actual social networking site, or other online. Con artists find it easy to create authentic-looking websites, and to send e-mails or instant messages from addresses that seem genuine. The website may ask you to type in your username, password, credit card number, or other personal data.

Kevin Mitnick, once a notorious computer criminal and now a security consultant, summed up in an August 29, 2011 interview with TIME the ways criminals combine social engineering and plain old psychological trickery with computer hacking skills.

A hacker might learn your likes and dislikes from your posts on Facebook or another social website. Perhaps, like many adults, you’ve gotten hooked on the video game “Angry Birds” because your grandchildren enjoy playing it on granddad’s smart phone. “If I know you love Angry Birds, maybe I would send you an e-mail purporting to be from Angry Birds with a new pro version. Once you download it, I would have complete access to everything on your phone,” Mitnik told the magazine.
How can you protect yourself when any e-mail may be a “phishing” hook? Very simply: Never do what an e-mail, text message, or website tells you to do—never click on a link or download an attachment without checking to make sure it’s genuine. Find a contact number for the organization that supposedly sent the e-mail or maintains the website. Be careful, since some criminals have been known to set up messaging accounts for “live chat assistants,” to convince victims a fake website is real. Protecting yourself in this way is worth the time and effort.

Further notes on Internet Safety—When choosing an e-mail address or screen name, don’t reveal personal information. An address with random characters, such as “nab197”, is better than one stating your age and hometown, like “woodbridge1954.” Choose a password that isn’t easy to guess—the more complex the better—and keep it written somewhere safe in case you forget it!

Conduct research before you buy anything online—especially from sites where strangers sell to each other. Be sure you know what you’re purchasing. Know all of the terms of the sale, including return policies and shipping costs. Verify the seller’s physical address and phone number. Look online for customer reviews or complaints about the seller.
A word about online dating. **Don’t give your address or other personal information to anyone you don’t know.** Never loan money to someone you met online. Remember there’s no such thing as a private photo on the Internet; if you post it, someone can copy and send it. **If you choose to meet someone, meet for the first few times in a public place, and let a friend know where you’re going and whom you will be meeting.**

**IMPOSTOR SCAMS**

**The “Grandparent Scam:”** “Grandpa, it’s me! I was drinking and got in an accident. Now I’m calling you from jail and need bail money. Please go to the Western Union office and send me $2,000 right away! And please don’t tell mom; she’ll be so disappointed!”

**The “Friend-in-Trouble E-mail Scam:”** “This is your friend Tracy, e-mailing from London. John and I got mugged while traveling. We lost everything, and need cash for a flight home! If you wire us the money as soon as possible, I promise we’ll pay you back.”

**The “Foreign Investor Scam:”** “I am a high-ranking person in a foreign country, sending random e-mail to a total stranger. I must transfer funds to an American bank account. Please e-mail your account information to me, and together we will realize great profit!”
The “Bill Collector Scam:” “I am calling on behalf of XYZ Payday Loan Company. You may not remember ever doing business with us, but you owe us $2,000 and are in default. If you don’t pay right away we will take you to court and ruin your credit, and we may even refer this matter to the Attorney General for criminal prosecution.”

Each year, thousands of victims lose large sums of money— or even suffer identity theft— due to imposter scams like these.

The “Grandparent Scam” is relatively new. The scammer calls by phone, pretending to be the victim’s grandchild. Caught up in urgency and emotion, the victim sends a wire transfer for hundreds of dollars— only to learn, hours later, that their grandchild was never in trouble. By that time the money is gone, and may never be seen again.

The “Bill Collector” scam attempts to scare consumers by making them believe they will face terrible consequences, including expensive lawsuits, unless they pay a “debt” they don’t actually owe. Even if you actually are in default for a debt, federal law prevents bill collectors from harassing you or threatening you with criminal action. See page 32 of this book for more on your rights under the Fair Debt Collection Practices Act.
These scammers do their homework. They use “social engineering” tricks like those described in the “Phishing” section of this book. They purchase marketing lists with the names and phone numbers of senior citizens, or they hack into e-mail accounts, and send “help!” messages to everyone in the person’s contact list.

To sound truly convincing, someone pretending to be your grandchild or friend may mention your hometown or the names of other people you know—details easily found online, in obituaries or on social networking sites like Facebook. They will tell an elaborate story, and have answers for every question you ask, or they may trick you by saying, “Hello, Grandpa?” in a muffled voice. When you reply, “Is that you, John?” you’re unwittingly providing the name of your grandchild.

Almost always, they will ask you to send money through Western Union or a similar wire service. Protect yourself by staying alert.

Never wire money without being absolutely sure you know who will pick it up. Never send bank account or credit card information to someone who says you’ll get a reward. If you receive an emergency call asking for money, always check with a family member to find out whether your loved one really needs help.
Talk with your family about these scams. Consider creating a secret phrase—something only the family would know—in case it becomes necessary to make an emergency call for help.

ONLINE BUYING and SELLING SCAMS

It is not possible to predict every scam the world’s con artists will create and use. But studying the real scams described here can help you recognize a few basic patterns and protect yourself when someone offers a deal that’s too good to be true, or tells you a story that doesn’t quite add up.

*The Online Sale scam:* The scenario— you’d like to buy a good, used car online. While scanning various for-sale-by-owner ads, you see an attractive vehicle on sale for a fraction of its normal value. You reach out to the owner, who tells you by e-mail she’s offering the car for such a low price because she found a new job after having been unemployed. She must relocate, and can’t take the car with her. She says she’s extremely busy, won’t be able to meet you and won’t give you a chance to inspect the car. But she’s in a rush, and wants you to make a decision right away. She tries to make the deal sound reassuring. Even though the car was not offered on eBay Motors, she tells you the sale will be protected by the eBay Motors Vehicle Protection Plan (VPP). She even sends you a link to a website with a *live-chat*
feature, in which you exchange instant messages with a “live-chat assistant” who says there are safeguards in place to reimburse you for any loss. Finally you agree, and send money by wire transfer for the car and the cost of delivering it to your house. Weeks and months go by. Your money is gone and the car never arrives.

This is an elaborate and well-thought-out scam. The criminals create attractive deals by selling cars at prices below book value. They misuse the names of well-known companies and programs – such as the eBay Motors VPP, a reputable protection program whose name is often hijacked by these con artists. However, the VPP is not applicable to transfers that originate outside of eBay Motors, and it prohibits wire transfer payments. They even use a live-chat feature that makes you believe you’re speaking with a third-party assistant.

Beware of sellers who want to move the transaction from one platform to another (for example, from eBay Motors to Craigslist). Beware of sellers who claim that a buyer protection program, offered by a major Internet company, will cover a transaction conducted outside that company’s site. Never trust sellers who push for speedy completion of the transaction. Beware of transactions where the seller and vehicle are in different locations (for example, because the “seller” had a job transfer, is deployed by the military, or moved for family reasons). Be
suspicious if vehicles are being advertised at well below their market value. Remember, if it looks too good to be true, it probably is. In addition, beware of sellers who request payments via wire transfer services such as Western Union.

**The Cashier’s Check scam:** The scenario: You’re seeking to sell your old dining room furniture. You offer it for sale on Craigslist for what you hope is a reasonable price—say, $400. Soon a potential buyer sends an e-mail, offering $700. He says he’s willing to pay more just to make sure you don’t sell it to anyone else. He says he won’t be able to come and inspect the furniture, and will have to conduct the entire transaction via e-mail, because he’s overseas on a military deployment. But that doesn’t matter, because a military liaison will pick up the furniture and deliver it to his family’s house once the transaction has been completed.

You were afraid people would haggle for a lower price, but here’s a poor young American soldier begging you to overcharge him. It sounds like a great deal, so you accept his offer. There is one catch: For some reason that doesn’t quite make sense, his bank can only send you a cashier’s check for $1,000. He asks that you deposit the check into your account, then send a wire transfer for $300 to his relative in another state. When you deposit his cashier’s check, the $1,000 appears to be credited to your account, so you make the wire transfer. But there is
no further communication from the young soldier. A few days later, your bank informs you the $1,000 check was a fake, and the money initially credited to your account has vanished. You were conned out of $300.

This is an elaborate ruse that preys on your hope to make money—and your assumption that a cashier’s check is as good as cash. Unfortunately, that is not the case. When you deposit a cashier’s check, your bank may immediately credit the funds to your account—but, since the actual bank-to-bank transaction takes a few days, a fake cashier’s check won’t be detected right away. There is just enough time for you to get ripped off, while you think the money is secure in your bank account.

Beware of buyers who offer to purchase your goods for a price higher than the price you’ve offered. Once again, if it looks too good to be true, it probably is. Also, beware of buyers who are in a rush, and who are not interested in getting to know you or inspecting the merchandise before they pay. Many con artists will say they can’t meet you because they’ve been deployed by the military, are overseas for a vacation or a job, or are moving for family reasons.
This chapter does not cover every possible scam. But your awareness of them will help you protect yourself. Discuss these scams with your loved ones, and keep them in mind every time you conduct a transaction or are asked to send someone money.

**SWEEPSTAKES and TELEMARKETING SCAMS**

Not every sweepstakes, and not every telemarketer, is a fraud. Many sweepstakes are run by reputable organizations to promote their services. Some contestants even win a prize. Likewise, many telemarketers seek to sell an honest product or service.

However, many scams come disguised as sweepstakes, telemarketing calls, and Internet ads. Always remember, if it sounds too good to be true, it probably is.

**Signs of a Sweepstakes Scam:**

- Mailings or online ads that say you must buy something to win.
- Ads that say you must respond “NOW!” or forfeit your chance of winning.
- Ads that say a contest is endorsed by state or federal government, or say you’re part of a “select group.”
- Ads that say you’ve already won— but you must send money to claim your prize.
Never, ever send money to claim a prize. Never give your credit card, Social Security number, or other personal information to someone who says you’ve won a prize.

Telemarketing and the Do-Not-Call List: You can put your phone numbers on the national Do Not Call Registry at 888-382-1222, or www.donotcall.gov, to prevent telemarketers from calling. Never allow a caller to pressure you into acting immediately on any offer. Never agree to any offer unless you have seen it in writing. Never give your credit card number, Social Security number, or other personal information to a telemarketer.
Chapter 3-protecting your identity and credit
Identity theft is considered the fastest-growing financial crime. It occurs when a thief assumes the victim’s identity in order to make purchases or apply for credit or other benefits in the victim’s name. The victim whose identity has been stolen can suffer adverse consequences—such as a ruined credit history—if he or she is held accountable for the identity thief’s actions.

How do these thieves hijack your “identity”? It can happen through phishing (see page 13), in which criminals trick victims into handing over their online passwords, usernames, or credit card numbers. It can also be as easy as stealing your driver’s license, credit card, or other identifying documents. Either way, you should follow basic, regular steps for self-protection:

- Start by keeping a list of your account numbers, credit card numbers, PINs, and the phone numbers of your creditors.
- Carefully review your bank statements and bills. Contact your creditors if you notice any unauthorized activity, or if your bills do not arrive on time.
- Pay attention to invoices and billing statements from businesses with whom you don’t
have an account. This “mystery mail” may be a sign that a scam artist has used your personal information to obtain goods and services.

- Never give personal information over the phone, unless you initiated the call and are providing it to a company you know and trust. If making a purchase online, do not give your credit card number unless you have verified that the site is valid, and is controlled by a company you trust. Shred all mail that has personal or account information before disposing of it.

- Check your credit reports on a regular basis. You can obtain one free credit report every 12 months from each of the three credit reporting bureaus, by calling 877-322-8228 or visiting www.AnnualCreditReport.com.

If you believe you have been victimized (if your wallet, credit cards, or checks are stolen), report the theft to police and request a police report. You can use the police report when writing to credit card companies, utilities, and other businesses as evidence that any unauthorized charges were made by someone else.

- Remember to cancel your credit and debit cards. Notify your other creditors, and send them
protecting your identity and credit

If you have been victimized, be sure to contact one of the three credit reporting bureaus and file a fraud alert. Fraud alerts let vendors know you may be a victim of identity theft, and that your identity should be verified before new credit is issued in your name. Review your credit report periodically, and report any suspicious activity to the credit reporting bureaus.

- Consider asking the credit bureaus to place a freeze on your credit report. This will block potential creditors from accessing your credit information, and make it difficult for identity thieves to open new credit cards or obtain loans in your name. However, if you need to have your credit checked in order to obtain a loan, or for any other purpose, you would need to contact all three credit bureaus to lift the credit freeze in advance.

The three credit reporting bureaus are:
- Equifax, 800-525-6285, www.equifax.com;

- If you’re getting rid of a computer, smart phone or other electronic device, make sure to
completely erase its memory! Simply moving items to “trash” is not enough to truly erase all of the banking data, tax reports, photos, and other personal information hidden in your device’s hard drive. Before you sell or recycle these devices, talk to the manufacturer and learn how to securely and completely remove all your old data.

CREDIT and DEBT

Credit affects your power as a purchaser. Your credit score can affect your ability to buy a home or car, obtain a student loan, mortgage or credit card, rent an apartment, or apply for a job.

Check your credit reports on a regular basis; this is essential to maintain good credit or help repair bad credit. You can obtain one free credit report every 12 months from each of the three credit reporting bureaus, by calling 877-322-8228 or visiting www.AnnualCreditReport.com.

If you notice any errors on your credit report, contact the reporting bureau immediately. The bureau will then have 30 days to investigate and must inform you of its findings within 10 days of concluding the investigation.

If a credit reporting bureau fails to provide a free copy of your credit report, or to investigate
protecting your identity and credit

and correct inaccurate information, contact the New Jersey Division of Consumer Affairs. If you have bad credit, you can take action to improve it. But this requires time—negative information will remain on your credit history for seven to 10 years—and your timely repayment of debt.

If you are experiencing difficulty paying your bills, contact your creditors immediately. Try to work out a payment plan before the bills are sent to a collection agency.

If you believe a bill is inaccurate, write to the company. It’s best to send your inquiry by certified mail, and request a return receipt from the Post Office. Include your name, account number, the dollar amount in question, and the reason you believe the bill is wrong. Send a copy of the sales receipt and any other documents. Never send originals, as it may take more than one letter to correct the problem.

Beware of anyone who offers instant solutions to credit problems. Instant solutions don’t exist, and many con artists seek to prey on those who feel desperate because of financial troubles. Some may offer to “hide” your bad credit by establishing a new credit identity with a fake Social Security number. Needless to say, this is fraud, and it is a crime!
Under the federal **Credit Repair Organizations Act**, credit repair organizations **cannot charge money up-front for any service, before it is fully performed**. Before you sign a contract with a credit repair organization, it must provide a document explaining your “**Consumer Credit File Rights**.” Credit repair organizations cannot provide services without a written and dated contract. The consumer may cancel the contract within three business days after signing. Any contract that does not comply with the laws, is void.

Be very careful if you choose to work with a debt adjuster. Contact the **New Jersey Department of Banking and Insurance** to find out whether the person is licensed, or otherwise legally authorized, to perform debt adjustment services. Unlicensed, fraudulent operators may take your money and vanish, without performing the services for which you paid. Too many New Jersey consumers have been scammed in this way.

If you’re looking for a nonprofit counseling program, check with universities, military bases, credit unions, housing authorities, and branches of the U.S. Cooperative Extension Service.

**A note about debt collectors.** The **Fair Debt Collection Practices Act (FDCPA)** applies to personal, family, or household debts. It specifies that debt collectors may not harass
protecting your identity and credit

debtors; may only contact them between 8 AM and 9 PM; may not lie in the effort to collect a debt, such as falsely implying the debtor has committed a crime; may not call debtors at work if they know the employer disapproves; and must stop contacting the debtor, if the debtor asks them to do so in writing. NOTE: Don’t fall for the “Bill Collector Scam” (see page 17 of this book), in which fraudulent debt collectors try to scare victims into paying “debts” they don’t actually owe.

If you believe your rights have been violated—by a creditor who refuses to work with you on a billing dispute, by a credit counselor, or by a debt collector—contact the New Jersey Division of Consumer Affairs.
Chapter 4 - Investments and Mortgages
INVESTMENT and SECURITIES FRAUD

The list of potential investment and securities scams is constantly changing. By studying today’s scams, you can develop the awareness to protect yourself against those scams a con artists might try to sell you tomorrow.

A few things are always true. Scammers follow the news and seek to exploit the headlines to their advantage. They make questionable claims, such as “Earn 25 percent, guaranteed!” and “Invest in foreclosed homes and make a fortune!” They offer the opportunity to get in on the ground floor of new technology and new ideas.

The basic advice for consumers is relatively simple. Before making an investment, contact the New Jersey Bureau of Securities, within the Division of Consumer Affairs, at 866-I-Invest (866-446-8378) and ask whether the investment opportunity and the person selling it has the appropriate registrations. The Bureau of Securities can also tell you about the person’s employment history, educational background, and additional information to help you make an informed decision.
Choosing a reputable firm and agent are important, as are the following additional steps.

Before signing any agreement or form, ask questions to be sure you understand the investments, investment strategy, and the names of the companies issuing the securities.

Ask about any fees or commissions, and ask about the maturation dates of bonds or certificates of deposit.

Press for full disclosure and the meaning behind all designations and titles, such as the credentials of the individuals with whom you are dealing. Check with the Bureau of Securities about a person’s purported credentials. It is illegal to use fake credentials or misleading designations that can convey to the public a level of education or accreditation that does not exist.

Get everything in writing and take notes of what was said, decided, and agreed upon.

Beware of high-pressure tactics, including claims that an investment is “safe,” “guaranteed,” or otherwise too good to be true. Beware of affinity fraud, in which scam artists try to make victims feel comfortable by playing up their membership in the same church, organization or ethnic group.

**Top 10 Investment Scams**—The Bureau’s website, in partnership with the North American Securities Administrators Association (NASAA), also includes the annually updated list of “Top 10 Investment Scams.” Though some details change, the same scams keep popping up year after year, evidence that the same old schemes are good at hooking new victims. The current list includes:

10. **Speculative Inventions and New Products.** New products are for venture capitalists who know how to assess the risks. They are not good investments for your retirement money even though they may promise high returns.

9. **Short-Term Commercial Promissory Notes.** Many seniors have lost their life savings by investing in short-term commercial promissory notes that are nine months or less in duration. These notes may be touted as being “insured” or “guaranteed,” but the insurance companies generally are located outside of the United States, are not licensed to do business in the United States, and lack the resources necessary to deliver on the promised guarantees.

8. **Real Estate Investment Schemes.** Members of NASAA have noted a rise in scams
disguised as offers to help homeowners who are caught up in the turbulent housing market “save” their homes or “fix” their mortgages, usually in exchange for a fee paid in advance.

7. Private Placement Offerings. Private placements offer businesses the opportunity to raise capital by selling securities to a relatively small number of investors as opposed to a public offering made through national securities markets. State securities regulators have observed a steady and significant rise in the number of private placement offerings that are later discovered to be fraudulent, especially those made under a federal registration exemption (Regulation D, Rule 506).

6. Ponzi Schemes. Despite the heightened awareness of Ponzi schemes following Bernard Madoff’s multibillion dollar fraud and 150-year prison sentence, these scams continue to trap investors.

5. Natural Resource Investments. NASAA expects to continue to see a rise in energy and precious metals scams promising quick, high returns, as well as fraudulent offerings of investments tied to natural gas, wind and solar energy, and the development of new energy-efficient technologies.
4. **Securitized Life Settlement Contracts.** Life settlement contracts are investments in the death benefits of an unrelated, third party’s life insurance policy. Legitimate investments of this kind involve a high degree of risk. Investors may be on the hook for routinely paying costly premiums, if the insured person outlives his or her life expectancy. Aside from the legitimate offerings, many crooks have developed fraudulent, “securitized” life settlement contracts in which bonds or other securities will supposedly guarantee a fixed return on a fixed rate, regardless of when the insured person dies. This supposed, risk-reducing structure has too often proved fraudulent, and left victims with worthless paper issued by a bonding company that does not maintain sufficient assets or does not exist.

3. **Leveraged Exchange-Traded Funds (ETFs).** This relatively new financial product has been offered to individual investors who may not be aware of the risks these funds carry. The funds, which trade throughout the day like a stock, use exotic financial instruments, including options and other derivatives, and promise the potential to provide greater than market returns as the value of the underlying assets rises or falls. Given their volatility, these funds typically are not suitable for most retail investors.

2. **Gold Bullion and Currency Scams.** With the high price of gold, investors should beware
of gold bullion scams. Similar to those are the many forms of foreign exchange (FOREX) trading schemes. Promoters profit by charging high commissions or selling investment strategies assuming that trades are actually made. In many instances there are no trades; the money is simply stolen.

1. **Entertainment Investments.** These unregistered investments, encompassing a variety of products including movies, infomercials, Internet gambling and pornography sites, promise high returns while offering little disclosure of risk.

**MORTGAGE SCAMS**

If you’re seeking to buy a home, or if you are a financially distressed homeowner trying to keep from losing your home, it is all too easy to fall prey to deceptive business practices. Scammers know your anxiety and fear may prevent you from looking closely at an “amazing” offer. Arm yourself by becoming aware of the following scams.

**Deceptively advertised mortgages and predatory lending—** In the first decade of the 21st century, banks sold thousands of “Pick-a-Payment” adjustable rate mortgages along with other deceptive loan products, by touting their low monthly payment options. But they failed to warn borrowers that choosing the minimum payment option could lead to a treadmill of debt. The
"low" monthly payments often did not cover the interest on the loan, which led to an increase in the loan’s principal balance and caused the monthly payment to spike well beyond what the consumers expected or were able to pay. Many borrowers became delinquent and subsequently lost their homes.

Protect yourself by never signing a mortgage contract without reading it thoroughly, and by being certain that you understand the full terms of the loan. Remember to ask about hidden costs, late fees, and whether the interest or principal rates might increase. Be sure you know the full amount you will pay each month, along with the interest rate, and whether it’s affordable. If the person selling the loan won’t provide straight answers or clear information, just walk away.

**Mortgage loan modification scams:** If you’re hit by financial hardship and are struggling to pay your loan, there are legitimate ways to try to negotiate a more affordable monthly payment. Not everyone who offers to help with a “mortgage loan modification” is legally authorized to do so. Debt adjusters are required to obtain licensing through the New Jersey Department of Banking and Insurance. The unlicensed, fraudulent operators may take your money—sometimes an entire mortgage payment—and vanish, without ever performing the services for which you paid. Too many New Jersey homeowners have been scammed in this way.
You must do all you can to protect yourself. You can seek to negotiate a mortgage loan modification yourself, by calling the lender and explaining your situation. If you need help, ONLY work with someone legally authorized to perform mortgage loan modification work. The ONLY people authorized to do so in New Jersey are nonprofit debt adjusters, licensed by the State Department of Banking and Insurance (DOBI); the lender or owner of the loan; a mortgage servicer acting on the lender’s behalf; or a lawyer, provided he or she is not primarily engaged in debt adjustment. For a list of licensed mortgage adjusters, call DOBI at 800-446-7467.

Beware of anyone who asks you to pay a large, up-front fee (such as one month’s mortgage payment) for help with a mortgage loan modification. Be suspicious of anyone who tells you not to contact your lender because, “I’ll handle the details for you.” In addition, beware of anyone who asks you to make future payments to a new person or firm, without contacting your current mortgage lender.

Foreclosure scams: Homeowners facing foreclosure are often the target of scams. Someone may offer to buy your home at much less than its actual value, then let you lease the home, claiming you’ll eventually be able to buy it back. To a desperate person this may sound decent—but such offers often make it impossible to buy back the home. You may gain a few thousand
dollars in the short term, only to lose tens of thousands in equity, in addition to losing ownership of the home.

Protect yourself by seeking legal advice only from a trusted attorney— not one recommended by a foreclosure company or individuals soliciting you to hire them. Never sign away ownership of your home without consulting your attorney. Beware of any home-sale contract in which the homeowner is not formally released from liability for the mortgage!

**Surplus funds scams.** If your home is foreclosed upon and sold at a sheriff’s auction, it may be sold for more than you owe on the mortgage and taxes. You may be entitled to those surplus funds, in some cases amounting to thousands of dollars. Unsurprisingly, scam artists will try to trick you out of those surplus funds.

Protect yourself. If your home is sold in a sheriff’s sale, call the sheriff’s office in your county to determine if the sale resulted in surplus funds. Contact the New Jersey Superior Court Trust Fund, at 609-292-4012, for help in applying for surplus funds. Avoid anyone who offers to help collect surplus funds for a fee; you can do it yourself for less than $100.
Chapter 5 - managing your health

New FedUp

Prevent Prescription Drug Abuse
Be Smart with Your Medications
Choosing a Doctor
In-Home Care
SHIP and AAA's
PREVENT PRESCRIPTION DRUG ABUSE

For too many New Jersey teenagers, addiction begins in the medicine cabinet. The State Commission on Investigation announced in 2011 that an alarming number of New Jersey teenagers experimented with pain drugs from family medicine cabinets, became addicted, and moved on to illicit drugs such as heroin. “Today’s young Percocet, Vicodin, and OxyContin users are becoming tomorrow’s heroin junkies,” an SCI official said in June 2011. “The demand for those drugs has spawned new levels of crime and violence.”

The number of Americans who abuse prescription drugs is greater than those who use cocaine, hallucinogens and heroin combined, according to the 2009 National Survey on Drug Use and Health. Teens who abuse prescription drugs often steal them from relatives.

The State Division of Consumer Affairs is taking strong steps to prevent the diversion and abuse of prescription drugs. The Division maintains New Jersey’s Prescription Drug Monitoring Program, which gathers information about prescriptions filled at New Jersey pharmacies to help identify “doctor shopping” and “pill mills” that make drugs available for abuse. The Division is launching a statewide “Prevent Prescription Drug Abuse” awareness campaign.
to educate health care professionals, patients, parents, and young people, and is also sponsoring Drug Take-Back Day events during which consumers are encouraged to turn in their unused or expired medications for safe disposal. For more information go to: www.NJConsumerAffairs.gov/PrescriptionDrugAwareness.

As a responsible citizen, you can help by properly disposing of your unused medicine. You don't have to wait for a Drug Take-Back Day. The FDA and White House Office of National Drug Policy offer the following advice:

Follow any specific disposal instructions on the medication’s drug label included in the patient information. Do not flush prescription drugs down the toilet unless this information specifically instructs you to do so. If no instructions are given on the label, you can throw drugs in the household trash. First, take them out of the original containers and mix them with an undesirable substance such as coffee grounds or kitty litter; then put the unattractive mixture in a sealable bag, empty can, or other container to prevent it from leaking out of a garbage bag.

Before throwing out a medicine container, scratch out all identifying information on the label; this will protect your identity and your privacy.
DO NOT give medications to friends. Doctors prescribe drugs based on a person’s specific symptoms and medical history. A drug that helps you may harm someone else. When in doubt about the proper means of disposal of a drug, talk to your pharmacist.

BE SMART WITH YOUR MEDICATIONS

Money-saving tips: The New Jersey Prescription Drug Price Registry, at www.NJDrugPrices.nj.gov, maintained by the Division of Consumer Affairs, lets consumers compare the prices offered at different pharmacies for the 150 most-frequently-prescribed medications. You can input the prescribed medication and dosage type, and your town name or ZIP code, for a list of prices reported by specific pharmacies in the area. Actual prices may vary, so you should call the pharmacy to learn the current price before buying.

Why is this important? Prescription drug prices can vary as much as $60 per unit from one New Jersey pharmacy to the next.

But be careful, and always talk to your pharmacist. Consumers buying prescription medications—especially if they buy from more than one pharmacy—must communicate with the pharmacist about their medical condition and the full list of drugs they are taking.
Failure to do so may result in purchasing drugs that are not compatible with each other, or in combination can be dangerous to the patient’s health.

You may also be able to save money by using generic drugs, or asking about drugs that are therapeutically similar to more expensive drugs that have been prescribed for you. Speak with your health care provider and your pharmacist to find out if this would be a safe option.

**Safety tips**— First and foremost, read the “PREVENT PRESCRIPTION DRUG ABUSE!” section of this booklet, and learn how to properly dispose of your unused medications.

**Additional tips**— Before using any medication, be sure you know exactly how it should be taken. Ask the pharmacist, who is required to offer to speak with you. Read the labels completely and follow all of the directions. Be sure you know how, when, and for how long you should take the medicine. Know whether there are restrictions regarding food, drink, or other medications. Find out whether you may be allergic to the medication. Know what to do if you miss a dose, and how the medicine should be stored. Failure to follow these instructions can result in severe reaction or death.
Never give medications to a friend, or accept medications from a friend, even if you have the same symptoms. Doctors prescribe drugs based on a patient’s specific symptoms and medical history. A drug that helps you, may harm someone else.

**Information on Pharmacies**—Pharmacists in New Jersey are licensed by the Division of Consumer Affairs. Your pharmacist is required to counsel you about medications prescribed by your doctor, and to maintain a patient profile on all customers. The profile enables the pharmacist to identify medications you are currently taking when a new prescription is filled, determine whether there could be a negative interaction between new medications and other drugs or the patient’s allergies, and to guard against possible misuse of the prescription. Pharmacists are also required to enter information about prescriptions they sell, into New Jersey’s Prescription Drug Monitoring Program, to help law enforcement identify warning signs about the diversion and abuse of prescription medications.

When purchasing medication, it is always important to talk with your pharmacist about your medical condition, the full list of drugs you are taking, and any allergies you may have. Failure to discuss this may result in purchasing drugs that are not compatible with each other, or in combination can be dangerous to your health.
Online Pharmacies—You should be very careful if you consider ordering drugs from an online pharmacy—The Division of Consumer Affairs and the National Association of Boards of Pharmacy (NABP) require online pharmacies to comply with the licensing and inspection requirements of the state in which they are located, and in all states to which they dispense medications. To help consumers identify safe sites, the NABP developed the VIPPS (Verified Internet Pharmacy Practice Sites) accreditation program. Consumers should look for the VIPPS seal on an accredited site, or check NABP’s database of accredited online pharmacies at www.vippspharmacies.net.

The NABP in July 2011 found that 96 percent of 8,000 rogue pharmacy websites continue to operate out of compliance with United States pharmacy laws, and provide an outlet for counterfeit medicines to enter the drug supply. Some drugs sold by unlicensed online pharmacies have been proven to be contaminated or outdated, to have no active ingredient or the wrong ingredient, or to contain products banned in the United States. Many online pharmacies are located overseas. There is no guarantee the person on the other end of the computer is a pharmacist, no guarantee the drug you receive is what the seller says it will be, no guarantee that what you buy is right for you, and no one you can contact if something goes wrong.
CHOOSING A DOCTOR

New Jersey’s Health Care Profile Website, at www.NJDoctorList.com, is maintained by the Division of Consumer Affairs and provides regularly updated information on approximately 32,000 medical practitioners in New Jersey. It helps consumers make informed decisions when they choose a medical doctor, podiatrist, or optometrist.

Consumers can access the list to look up specific practitioners by name. The listing on each practitioner includes, among other things: educational information including medical schools attended, degrees earned, and board certifications; legal actions, including whether the practitioner has made malpractice payments within the last five years, has been subject to disciplinary actions within the last 10 years, or has been subject to license limitations; practice information, including office locations, accessibility to persons with disabilities, and languages other than English, and whether the practitioner accepts Medicare or Medicaid.

For more information about a practitioner’s license status or disciplinary history, you can contact the Division of Consumer Affairs.
Be sure your medical practitioner is properly licensed by the State of New Jersey. Call the Division of Consumer Affairs if you’re not sure. Patients who were treated by unlicensed “doctors” or “dentists” have suffered horrific infections, broken teeth that were not fully extracted and other complications resulting in hospitalization. During 2010 and 2011 the Division of Consumer Affairs worked with local law enforcement on the arrests of approximately 20 individuals who chose to put the public’s health at risk by practicing medicine or dentistry without a license, or with a revoked license.

Here are a few tips when you are going to see your doctor. Make a list of the concerns you would like to discuss during your visit. Write down your entire health history, including past and present medical conditions. Bring the full list of medications you are taking, including dosages, the conditions for which you are taking them, and the physicians who prescribed them. Ask questions until you clearly understand the doctor’s opinions and advice. Don’t be afraid to ask how much treatments will cost. Be sure you know what your insurance will or will not cover. Ask about the cost differential between in-network providers and out-of-network providers.
IN-HOME CARE

Certified Homemaker-Home Health Aides (CHHHAs) provide in-home care under the supervision of registered nurses. A CHHHA may remain in the home on a 24-hour basis or less, and may divide the 24-hour day into shifts with other CHHHAs from the same home care agency. Generally speaking, CHHHAs provide the most hands-on form of in-home care, including assistance with bathing, dressing, grooming, and other aspects of personal hygiene, and ambulation. Other professionals—such as licensed practical nurses, physical therapists, respiratory care therapists, or others—may provide more specialized types of care in the home.

If possible, learn about CHHHA services before a healthcare crisis arises. This will save time and money, and enable you and your family to better tailor services to the patient’s needs, if such help becomes necessary. You can obtain a free copy of our “Consumer’s Guide to Homemaker-Home Health Aides” by calling the Division of Consumer Affairs at 800-242-5846, or you can find it at www.NJConsumerAffairs.gov/hhh/.

There are simple ways to protect yourself or your loved one when working with a CHHHA. All health agencies that employ CHHHAs must be licensed either by the New Jersey
Department of Health and Senior Services, or by the Division of Consumer Affairs. A list of health care service firms, licensed by Consumer Affairs, can be found in the “Consumer’s Guide to Homemaker-Home Health Aides." Before working with any such agency, contact the Division of Consumer Affairs to make sure its license is still valid and to learn if the agency has been the subject of consumer complaints. Demand copies of the agency's written policies for patients, and its liability insurance policy. Take the time to ensure that you understand the specifics of your own insurance policy related to CHHHA coverage. Finally, before working with an individual CHHHA, contact the Division of Consumer Affairs to make sure that individual’s State registration is also in good standing.

It is also a good idea to contact the Division of Consumer Affairs and learn about the license status of other health professionals who provide services in the home.
SHIP and AAAs

The State Health Insurance Assistance Program (SHIP) provides free help to New Jersey Medicare beneficiaries who have problems with or questions about their health coverage. SHIP is a statewide program sponsored by the New Jersey Department of Health and Senior Services, with major funding from the U.S. Department of Health and Human Services’ Centers for Medicare & Medicaid Services. For information or assistance, call 800-792-8820 or visit www.state.nj.us/health/senior/ship.shtml.

An Area Agency on Aging (AAA) has been designated in each New Jersey county to serve as the primary entity responsible for developing comprehensive, coordinated systems of community-based services for older adults. To contact the AAA in your county, call 877-222-3737 or visit www.state.nj.us/health/senior/sa_aaa.shtml.
FedUp
ADDITIONAL RESOURCES

This FedUp booklet provides an important guide to consumer self-protection. It provides valuable information concerning protecting yourself when conducting business, how to avoid common scams, protecting your identity and credit, how to safely invest and apply for a mortgage, and the best ways to manage your health.

If you’d like to read more, the New Jersey Division of Consumer Affairs’ website provides a wealth of information at www.NJConsumerAffairs.gov.

The “Publications” link on the right side of the page lets you access our Consumer Briefs with detailed information on additional topics such as predatory towing, selecting a mover, buying furniture, and much more. It also lets you view current and archived editions of our ConsumerWise Newsletter. The main page lets you view Press Releases on the Division’s enforcement activities, and Consumer Alerts about recent scams, product recalls and safety tips.

Finally, consumers who believe they have been cheated or scammed by a business, or suspect any other form of consumer abuse, can call our Consumer Service Center hotline at 800-242-5846.