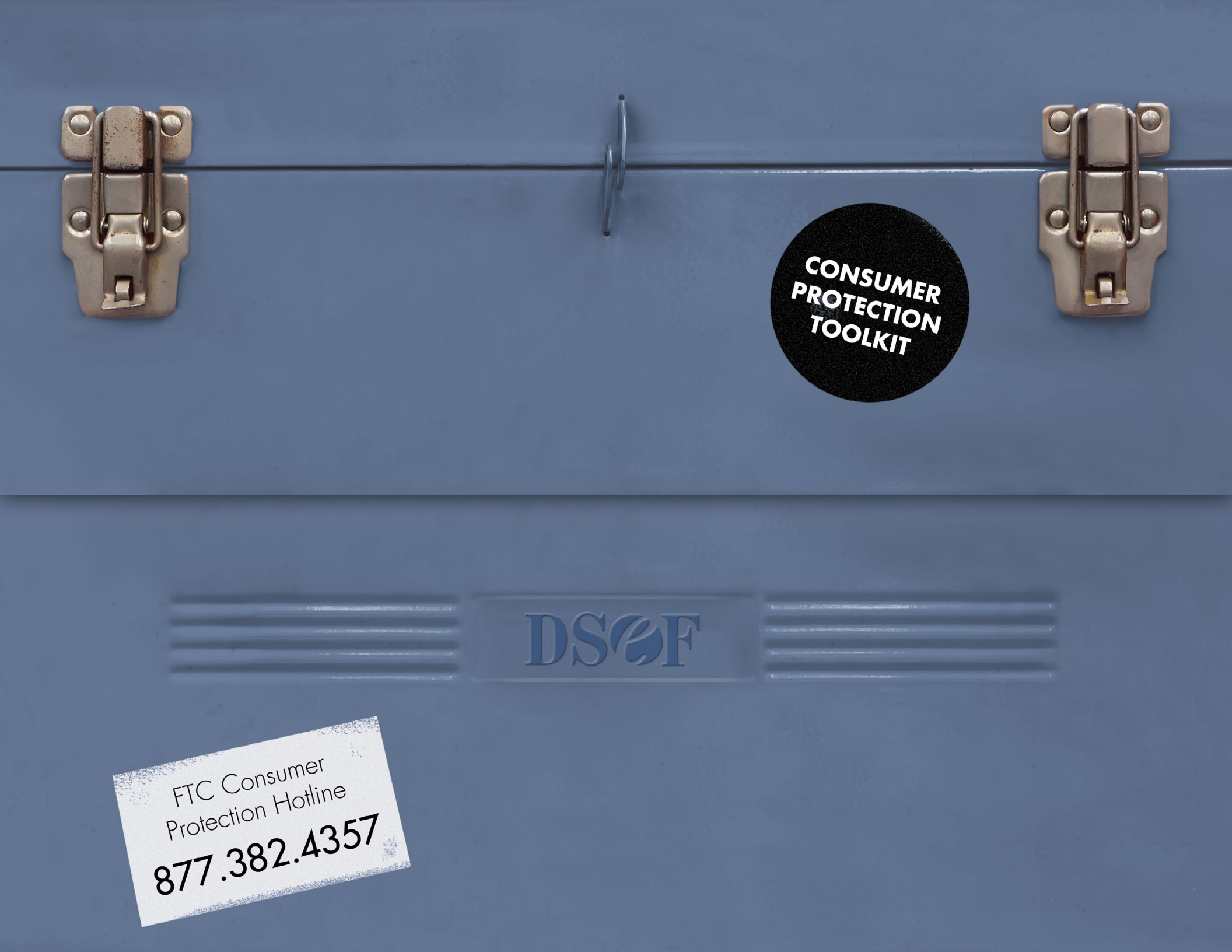

CONSUMER PROTECTION TOOLKIT
DSOF
FTC Consumer Protection Hotline
877.382.4357

TABLE OF CONTENTS

Consumer Protection 101

Additional Resources

CONSUMER PROTECTION 101

DSEF DIRECT SELLING EDUCATION FOUNDATION

John P. Parker
Amway
DSEF Chair

Gary M. Huggins
Executive Director

Dear Friend,

For more than 40 years, The Direct Selling Education Foundation (DSEF) has championed the rights of consumers around the world and advanced understanding of the direct selling channel through its partnerships with leading consumer advocacy groups, educators and public policy leaders.

As part of our support of consumer protection, we are pleased to introduce a consumer protection toolkit aimed at providing consumers with a one-stop-shop of information to help them avoid fraud and scams in the marketplace.

We hope you'll find the enclosed information valuable. For more educational resources visit www.dsef.org and www.ncpw.gov.

Sincerely,

Gary M. Huggins

DSEF DIRECT SELLING EDUCATION FOUNDATION

DSA/DSEF OVERVIEW

The Direct Selling Association (DSA) maintains a comprehensive Code of Ethics, detailing its member companies' commitment to ethical business practices and customer service. Educating consumers about these commitments is a core area of focus for the Direct Selling Education Foundation (DSEF). We invite you to learn more about our organizations:

DSEF

The Direct Selling Education Foundation (DSEF) is a national, non-profit organization that serves the public interest and advances understanding of the direct selling channel through partnerships, forums, education and research that showcase the industry's commitment to ethics, consumer protection and self-regulation. Visit www.dsef.org for more information.

DSEF DIRECT SELLING EDUCATION FOUNDATION

DSA

The Direct Selling Association (DSA) is the national trade association for companies that market products and services directly to consumers through an independent, entrepreneurial sales force. Nearly 17 million Americans are involved in direct selling in every state, Congressional district and community in the United States. In 2013, direct selling contributed more than $32 billion to the U.S. economy. Visit Direct Selling Facts at www.directsellingfacts.com for more information.

DSA DIRECT SELLING ASSOCIATION

1667 K Street, NW, Suite 1100, Washington, DC 20006 • T: 202.452.8866 • F: 202.452.9015 • www.dsef.org

DSEF DIRECT SELLING EDUCATION FOUNDATION

DSA'S CODE AND CONSUMERS

The cornerstone of the Direct Selling Association's (DSA) commitment to ethical business practices and consumer service is its Code of Ethics. Every member company pledges to abide by the code's standards and procedures as a condition of admission and continuing membership in DSA.

DSA DIRECT SELLING ASSOCIATION

The DSA Code of Ethics speaks to both the consumer and the seller. It ensures that member companies will make no statements or promises that might mislead either consumers or prospective sales people. Pyramid schemes are illegal and companies operating pyramids are not permitted to be members of the DSA.

The DSA Code of Ethics is enforced by an independent code administrator who is not connected with any member company. The code administrator will do everything possible to resolve any complaints to the satisfaction of everyone involved, and has the power to decide on remedies. All member companies have agreed to honor the administrator's decisions.

The Direct Selling Association (DSA) is the national trade association for companies that market products and services directly to consumers through an independent, entrepreneurial sales force. Nearly 17 million Americans are involved in direct selling in every state, Congressional district and community in the United States. In 2013, direct selling contributed more than $32 billion to the U.S. economy. For more information, please visit www.dsa.org

DSEF DIRECT SELLING EDUCATION FOUNDATION

DSA DIRECT SELLING ASSOCIATION

As a consumer you should expect salespeople to:

- Tell you who they are, why they're approaching you and what products they are selling.
- Promptly end a demonstration or presentation at your request.
- Provide a receipt with a clearly stated cooling off period permitting the consumer to withdraw from a purchase order within a minimum of three days from the date of the purchase transaction and receive a full refund of the purchase price.
- Explain how to return a product or cancel an order.
- Provide you with promotional materials that contain the address and telephone number of the direct selling company.
- Provide a written receipt that identifies the company and salesperson, including contact information for either.
- Respect your privacy by calling at a time that is convenient for you.
- Safeguard your private information.
- Provide accurate and truthful information regarding the price, quality, quantity, performance, and availability of their product or service.
- Offer a written receipt in language you can understand.
- Offer a complete description of any warranty or guarantee.

As a salesperson, you should expect a DSA member company to:

- Provide you with accurate information about the company's compensation plan, products, and sales methods.
- Describe the relationship between you and the company in writing.
- Be accurate in any comparisons about products, services or opportunities
- Refrain from any unlawful or unethical recruiting practice and exorbitant entrance or training fees.
- Ensure that you are not just buying products solely to qualify for downline commissions.
- Ensure that any materials marketed to you by others in the salesforce are consistent with the company's policies, are reasonably priced and have the same return policy as the company's.
- Require you to abide by the requirements of the Code of Ethics.
- Safeguard your private information.
- Provide adequate training to help you operate ethically.
- Base all actual and potential sales and earnings claims on documented facts.

1667 K Street, NW, Suite 1100, Washington, DC 20006 • T: 202.452.8866 • F: 202.452.9015 • www.dsef.org

- Encourage you to purchase only the inventory you can sell in a reasonable amount of time.
- Repurchase marketable inventory and sales aids you have purchased within the past 12 months at 90 percent or more of your original cost if you decide to leave the business.
- Explain the repurchase option in writing.
- Have reasonable start-up fees and costs.

The Direct Selling Association (DSA) is the national trade association for companies that market products and services directly to consumers through an independent, entrepreneurial sales force. Nearly 17 million Americans are involved in direct selling in every state, Congressional district and community in the United States. In 2013, direct selling contributed more than $32 billion to the U.S. economy. For more information, please visit www.dsa.org.

Scam artists in the U.S. and around the world defraud millions of people each year. They use the phone, email, postal mail, and the internet to trick you into sending money or giving out personal information.

Here are 10 things you can do — or not — to stop a scam.

Report Scams

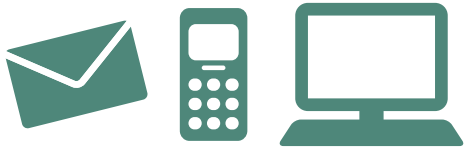
If you think you may have been scammed:

- File a complaint with the Federal Trade Commission at ftc.gov. If you are outside the U.S., file a complaint at econsumer.gov
- Visit ftc.gov/idtheft, where you'll find out how to minimize your risk of identity theft.
- Report scams to your state Attorney General. Visit naag.org.
- If you get unsolicited email offers or spam, send the messages to spam@uce.gov.
- If you get what looks like lottery material from a foreign country through the postal mail, take it to your local postmaster.

FEDERAL TRADE COMMISSION

August 2012

10 Ways to Avoid Fraud



FEDERAL TRADE COMMISSION

1 **Know who you're dealing with.** Try to find a seller's physical address (not a P.O. Box) and phone number. With internet phone services and other web-based technologies, it's tough to tell where someone is calling from. Do an online search for the company name and website, and look for reviews. If people report negative experiences, you'll have to decide if the offer is worth the risk. After all, a deal is good only if you get a product that actually works as promised.

2 **Know that wiring money is like sending cash.** Con artists often insist that people wire money, especially overseas, because it's nearly impossible to reverse the transaction or trace the money. Don't wire money to strangers, to sellers who insist on wire transfers for payment, or to anyone who claims to be a relative or friend in an emergency and wants to keep the request a secret.

3 **Read your monthly statements.** Scammers steal account information and then run up charges or commit crimes in your name. Dishonest merchants bill you for monthly "membership fees" and other goods or services without your authorization. If you see charges you don't recognize or didn't okay, contact your bank, card issuer, or other creditor immediately.

4 **After a disaster, give only to established charities.** In the aftermath of a disaster, give to an established charity, rather than one that has sprung up overnight. Pop-up charities probably don't have the infrastructure to get help to the affected areas or people, and they could be collecting the money to finance illegal activity. For more donating tips, check out consumer.ftc.gov.

5 **Talk to your doctor before you buy health products or treatments.** Ask about research that supports a product's claims — and possible risks or side effects. In addition, buy prescription drugs only from licensed U.S. pharmacies. Otherwise, you could end up with products that are fake, expired, or mislabeled — in short, products that could be dangerous to your health. Learn more about buying health products online at consumer.ftc.gov.

6 **Remember there's no sure thing in investing.** If someone contacts you with low-risk, high-return investment opportunities, stay away. When you hear pitches that insist you act now, that guarantee big profits, that promise little or no financial risk, or that demand that you send cash immediately, report them at ftc.gov.

7 **Don't send money to someone you don't know.** Not to an online seller you've never heard of — or an online love interest who asks for money. It's best to do business with sites you know and trust. If you buy items through an online auction, consider using a payment option that provides protection, like a credit card.

If you think you've found a good deal, but you aren't familiar with the company, check it out. Type the company or product name into your favorite search engine with terms like "review," "complaint," or "scam." See what comes up — on the first page of results as well as on the later pages. Never pay fees first for the promise of a big pay-off later — whether it's for a loan, a job, a grant or a so-called prize.

8 **Don't agree to deposit a check and wire money back.** By law, banks have to make funds from deposited checks available within days, but uncovering a fake check can take weeks. You're responsible for the checks you deposit: If a check turns out to be a fake, you're responsible for paying back the bank. No matter how convincing the story, someone who overpays with a check is almost certainly a scam artist.

9 **Don't reply to messages asking for personal or financial information.** It doesn't matter whether the message comes as an email, a phone call, a text message, or an ad. Don't click on links or call phone numbers included in the message, either. It's called phishing. The crooks behind these messages are trying to trick you into revealing sensitive information. If you got a message like this and you are concerned about your account status, call the number on your credit or debit card — or your statement — and check on it.

10 **Don't play a foreign lottery.** It's illegal to play a foreign lottery. And yet messages that tout your chances of winning a foreign lottery, or messages that claim you've already won, can be tempting. Inevitably, you have to pay "taxes," "fees," or "customs duties" to collect your prize. If you must send money to collect, you haven't won anything. And if you send any money, you will lose it. You won't get any money back, either, regardless of promises or guarantees.

4 WAYS DSA'S CODE OF ETHICS PROTECTS BUYERS & SELLERS

1 PRODUCT BUYBACKS

All DSA member companies must adhere to an inventory buyback policy.

2 COOLING OFF PERIOD

The cooling-off period protects consumers from buyer's remorse.

3 EARNINGS CLAIMS

Any claims a direct seller makes about earnings must be accurate and truthful.

4 PRODUCT CLAIMS

Any claims a direct seller makes about a product must be accurate and truthful.

To learn more about the Direct Selling Education Foundation's Ethics Initiative and the Direct Selling Association's Code of Ethics, visit www.dsef.org/what-we-do/ethics-initiative/

DSEF DIRECT SELLING EDUCATION FOUNDATION

1667 K Street, NW, Suite 1100, Washington, D.C. • 202-452-8866 • info@dsef.org • www.dsef.org

Shopping Online

Want to get a great product at a great price when you shop online? Some extra research can really pay off.

PLAN

Set a Budget

How much do you want to spend? Include delivery costs.

Decide What Matters

What are your "must-have" features vs. those that are nice to have?

COMPARE PRODUCTS

Use Search Engines

To find out more about a brand, product, or site, type the name into a search engine with words like "review," "complaint," or "scam."

Read Reviews Online

Reviews from other people, experts, and columnists can give you an idea of how a product performs. Don't put all your trust in any one review.

Consider Reputation

Does the brand or site have a reputation for quality and good customer service?

COMPARE COSTS

Check Shopping Comparison Sites

Some sites show the price of a product at several online stores. Keep shipping costs in mind when computing the best deal.

Consider Coupons

Coupon codes can impact your final costs. Do a search for the store with terms like "discount," "coupon," or "free shipping."

Read Return Policies

Not all stores have the same rules for returns. Some charge fees for return shipping or restocking.

CHECK OUT

Decide How To Pay

When you shop online, credit cards can offer extra protections.

Look for a Secure Checkout

Does the website address start with **https** (the "s" stands for secure) when you're checking out?

Learn more at **OnGuardOnline.gov/SmartShopper**

Job Scams

Scammers might promise you a job, lots of money, or work you can do at home. But they make you pay them before they help you. If you pay them, you will lose your money and will not get a job.

How do I spot a job scam?

Look for these signs of a scam. Scammers might:

- promise you a job
- promise you a government job
- offer you the secret to getting a job
- promise that you will make lots of money by working at home
- offer you a certificate to improve your chances of getting a job

Scammers **always** will ask you to pay first. That is the biggest sign of any scam. Never pay in advance. Someone might say you cannot lose. It is not true. You will lose money.

How can I avoid a job scam?

- Never deal with anyone who promises you a job. No one can **promise** you a job.
- Do not pay in advance for information about a job. Even if there is a money-back guarantee.
- Do not deal with anyone who says you have to act fast.
- Ignore promises to make thousands of dollars working in your own home. Those promises are lies.

What if I already paid someone but I did not get anything?

If you sent money and did not get help finding a job, report it to the Federal Trade Commission (FTC).

- Call the FTC at 1-877-382-4357
- Go online: ftc.gov/complaint

The FTC uses complaints to build cases against scammers. Any information you can give helps investigators.

ftc.gov
For The Consumer
Federal Trade Commission
1-877-FTC-HELP

FTC FACTS for Business

Ads for Business Opportunities:

How To Detect Deception

It's not hard to see why ads for business opportunities that promote the benefits of being your own boss and making money quickly are appealing. But the Federal Trade Commission (FTC), the government agency that monitors advertising for deception, says that some ads for business opportunities feature empty promises and false claims that potential entrepreneurs could never realize.

Promoters of fraudulent business opportunities run ads where their targets are likely to see them: in daily and weekly newspapers, in magazines, and on the Internet. The FTC is asking for your help in finding these ads first. By doing so, you can protect your company and your readers from being left holding the bag.

As part of an advertising sales or production staff, you customarily review ad claims for taste and appropriateness. It's just good sense to take that extra moment to review a business opportunity claim for telltale signs of fraud, too.

- It can protect your company from being known as one that promotes rip-offs. Your readers may believe an offer is legitimate because it's in your publication or on your website. When the claim turns out to be false, they may well blame you for running the ad.
- It can keep you from getting cheated by those who are making the false claims. There's a good chance they won't pay their bills, and will have left town by the time you try to collect.
- It can keep you from harming your readers and your legitimate advertisers.

Spotting False Claims

How can you spot claims for a fraudulent business opportunity? One clue may be the type of opportunity being advertised. Fraud has most often been associated with promotions for vending machine, display rack, pay phone, medical billing, and some Internet-related businesses.

Here are several other claims that have made it into the pages of legitimate papers, magazines and websites recently:

"WORK PART-TIME FROM HOME." Most scammers promise an ideal work situation — the ability to set your own hours, be your own boss, or work from home. In fact, this rosy scenario is far from reality for most small business owners.

"Be Your Own Boss" "Own a Dealership Today"

"EARN $2,000 A MONTH." If an ad claims buyers can make a certain amount of money, the law says the promoter must give the number and percentage of previous purchasers who earned the income. If an earnings claim is there, but the additional information isn't, ask for more information: the business opportunity seller may be violating the law.

"$50K/yr" "Vending route nets $1,700/wk"

"NO RISK! GUARANTEED!" Ads that promise a big payout with little or no risk are usually a telltale sign of a fraud. Legitimate business ventures involve risks — usually in proportion to the promised return.

"Huge Income" **"100% return on your investment!"**

"QUICK AND EASY!" Successful start-up businesses, including franchises, require a lot of work to get off the ground, let alone manage. Only a few are profitable from the start. If ads promise vending locations, they may not be current or high-traffic; the merchandise also may be out-of-date or of poor quality.

"Start Earning Today" **"Prime locations available now"**

These are examples of possibly deceptive claims. If you see them, highlight them for the appropriate person in your company. At the same time, know that many fraudulent business opportunity promoters use more subtle language when making promises, guarantees, and claims that they can't possibly keep.

By taking a few moments to review the claims made in business opportunity ads, you can protect the reputation of your company — and the consumers in your community.

For More Information

For information on red flag claims for weight loss products, visit ftc.gov/redflag. If you see an ad you think is deceptive, you can report it to the FTC using the complaint form at ftc.gov.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to sba.gov/ombudsman.

Federal Trade Commission	ftc.gov
1-877-FTC-HELP	For The Consumer

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer and Business Education

December 2006

DSEF DIRECT SELLING EDUCATION FOUNDATION

PYRAMID SCHEMES:

What you need to know to protect yourself from illegal scams

What is a pyramid scheme?

Pyramid schemes are illegal scams in which large numbers of people at the bottom of the pyramid pay money to a few people at the top. Each new participant pays for the chance to advance to the top and profit from payments of others who might join later. For example, to join, you might have to pay anywhere from a small investment to thousands of dollars. In this example, $1,000 buys a position in one of the boxes on the bottom level. Five-hundred dollars of your money goes to the person in the box directly above you, and the other $500 goes to the person at the top of the pyramid, the promoter. If all the boxes on the chart fill up with participants, the promoter will collect $16,000, and you and the others on the bottom level will each be $1,000 poorer. When the promoter has been paid off, his box is removed and the second level becomes the top or payoff level. Only then do the two people on the second level begin to profit. To pay off these two, 32 empty boxes are added at the bottom, and the search for new participants continues.

Each time a level rises to the top, a new level must be added to the bottom, each one twice as large as the one before. If enough new participants join, you and the other 15 players in your level may make it to the top. However, in order for you to collect your payoffs, 512 people would have to be recruited, half of them losing $1,000 each.

Of course, the pyramid may collapse long before you reach the top. In order for everyone in a pyramid scheme to profit, there would have to be a never-ending supply of new participants.

Things you should know about pyramid schemes

- Pyramiding is based on simple mathematics: many losers pay a few winners.
- They are fraudulent. Participants in a pyramid scheme are, consciously or unconsciously, deceiving those they recruit. Few would pay to join if the diminishing odds were explained to them.
- They are illegal. There is a real risk that a pyramid operation will be closed down by the officials and the participants subject to fines and possible arrest.

To look like a multilevel marketing company, a pyramid scheme takes on a line of products and claims to be in the business of selling them to consumers. However, little or no effort is made to actually market the products. Instead, money is made in typical pyramid fashion, from recruiting. New distributors are pushed to purchase large and costly amounts of inventory when they sign up.

The best way to avoid a disguised pyramid fraud is to know what to look for in a legitimate income opportunity.

Multilevel marketing—legitimate income opportunities

Multilevel marketing is a popular way of retailing in which consumer products are sold, not in stores by sales clerks, but by independent businessmen and women (distributors), usually in customers' homes.

As a distributor you can set your own hours and earn money by selling consumer products supplied by an established company.

In a multilevel structure you can also build and manage your own salesforce by recruiting, motivating, supplying and training others to sell those products.

Your compensation then includes a percentage of the sales of your entire sales group as well as earnings on your own sales to retail customers. This opportunity has made multilevel marketing an attractive way of starting a business with comparatively little money.

How to tell the difference between a legitimate business and a pyramid scheme

Pyramid schemes seek to make money from you (and quickly). Multilevel marketing companies seek to make money with you as you build your business (and theirs) selling consumer products. Before you sign up with a company, investigate carefully. A good way to begin is to ask yourself these three questions:

- How much are you required to pay to become a distributor?
- Will the company buy back unsold inventory?
- Are the company's products sold to consumers?

The start-up fee in multilevel companies is generally small (usually for a sales kit sold at or below company cost). These companies want to make it easy and inexpensive for you to start selling. Pyramid schemes, on the other hand, make nearly all of their profit on signing up new recruits. Therefore, the cost to become a distributor is usually high.

Pyramids often disguise entry fees as part of the price charged for required purchases of training, computer services, product inventory, etc. These purchases may not even be expensive or "required," but there will be considerable pressure to "take full advantage of the opportunity."

Legitimate companies which require inventory purchases will usually "buy back" unsold products if you decide to quit the business. Some state laws require buy-backs for at least 90% of your original cost.

How to protect yourself from a bad investment

1. Take your time. Don't let anyone rush you. A good opportunity to build a business in a multilevel structure will not disappear overnight. People who say "get in on the ground floor" are implying that people joining later will be left out in the cold. BEWARE!
2. Ask questions:
   - About the company and its officers.
   - About the products—their cost, fair market value, source of supply, and potential market in your area.
   - About the startup fee (including required purchases).
   - About the company's guaranteed buy-back of required purchases.
   - About the average earnings of active distributors.
3. Get written copies of all available company literature.
4. Consult with others who have had experience with the company and its products. Check to see if the products are actually being sold to consumers.
5. Investigate and verify all information. Do not assume that official looking documents are either accurate or complete.

Where to go for help

For help in evaluating a direct selling company, visit the Direct Selling Association at www.dsa.org, the Better Business Bureau at www.bbb.org, your local district attorney or your state attorney general.

If you suspect that a company may be an illegal pyramid scheme, contact your state and local law enforcement offices and the Federal Trade Commission at www.ftc.gov.

For more information about direct selling, visit www.directselling411.com. To find out more about ethical business practices, visit www.dsef.org

This brochure was originally published in cooperation with the National District Attorneys Association's Economic Crime Project.

1667 K Street, NW, Suite 1100, Washington, DC 20006 • T: 202.452.8866 • F: 202.452.9015 • www.dsef.org

Avoiding Identity Theft

Identity theft can make it hard for you to get credit, a job, a place to live, or utilities. But you can reduce your risk of being hurt by identity theft.

How can I protect my identity?

Protect your personal information. That helps you protect your identity. Here are some things you can do:

- At home
  - keep your financial records, Social Security and Medicare cards in a safe place
  - shred papers that have your personal or medical information
  - take mail out of your mailbox as soon as you can
- As you do business
  - only give your Social Security number if you must. Ask if you can use another kind of identification
  - do not give your personal information to someone who calls you or emails you
- On the computer
  - use passwords that are not easy to guess. Use numbers and symbols when you can
  - do not respond to emails or other messages that ask for personal information
  - do not put personal information on a computer in a public place, like the library

How will I know if someone steals my identity?

Read your bills and account statements. Watch for:

- things you did not buy
- withdrawals you did not make
- a change of your address that you did not expect
- bills that stop coming

Avoiding Identity Theft

Look at medical statements. You might see charges you do not recognize. That might mean someone stole your identity.

Get your credit report. You get one free credit report every year from each credit reporting company. To order:

- Call Annual Credit Report at 1-877-322-8228.
- Answer questions from a recorded system. You have to give your address, Social Security number, and birth date.
- Choose to only show the last four numbers of your Social Security number. It is safer than showing the full number on your report.
- Choose which credit reporting company you want a report from. (You get one report free from each company every year.)

The company mails your report to you. It should arrive two to three weeks after you call.

Read your credit report carefully. Look for mistakes or accounts you do not recognize. This could mean someone stole your identity.

Red Flags of Identity Theft

- mistakes on your bank, credit card, or other account statements
- mistakes on the explanation of medical benefits from your health plan
- your regular bills and account statements don't arrive on time
- bills or collection notices for products or services you never received
- calls from debt collectors about debts that don't belong to you
- a notice from the IRS that someone used your Social Security number
- mail, email, or calls about accounts or jobs in your minor child's name
- unwarranted collection notices on your credit report
- businesses turn down your checks
- you are turned down unexpectedly for a loan or job

Taking Charge:
What To Do If Your Identity Is Stolen
Available online at ftc.gov/idtheft
Order free copies at bulkorder.ftc.gov

FEDERAL TRADE COMMISSION
FTC.GOV/IDTHEFT
1-877-ID-THEFT (438-4338)

IDENTITY THEFT

WHAT TO KNOW

WHAT TO DO

FEDERAL TRADE COMMISSION
FTC.GOV/IDTHEFT

What is Identity Theft?

Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve. Identity theft happens when someone steals your personal information and uses it without your permission.

Identity thieves might:

- go through trash cans and dumpsters, stealing bills and documents that have sensitive information.
- work for businesses, medical offices, or government agencies, and steal personal information on the job.
- misuse the name of a legitimate business, and call or send emails that trick you into revealing personal information.
- pretend to offer a job, a loan, or an apartment, and ask you to send personal information to "qualify."
- steal your wallet, purse, backpack, or mail, and remove your credit cards, driver's license, passport, health insurance card, and other items that show personal information.

How to Protect Your Information

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months. To order, go to annualcreditreport.com or call 1-877-322-8228.
- Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan. If a statement has mistakes or doesn't come on time, contact the business.
- Shred all documents that show personal, financial, and medical information before you throw them away.
- Don't respond to email, text, and phone messages that ask for personal information. Legitimate companies don't ask for information this way. Delete the messages.
- Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address; "s" is for secure.
- If you use a public wireless network, don't send information to any website that isn't fully encrypted.
- Use anti-virus and anti-spyware software, and a firewall on your computer.
- Set your computer's operating system, web browser, and security system to update automatically.

If Your Identity is Stolen...

1 Flag Your Credit Reports

Call one of the nationwide credit reporting companies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days.

Equifax *1-800-525-6285*
Experian *1-888-397-3742*
TransUnion *1-800-680-7289*

2 Order Your Credit Reports

Each company's credit report about you is slightly different, so order a report from each company. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company.

3 Create an Identity Theft Report

An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report:

- file a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
- take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

The two documents comprise an Identity Theft Report.

ADDITIONAL RESOURCES

CONSUMER SENTINEL NETWORK
Law enforcement's source for consumer complaints

THE FTC'S CONSUMER SENTINEL NETWORK

A FREE online investigative tool from the Federal Trade Commission

- Search millions of consumer complaints
- Connect with thousands of law enforcers
- New and improved features make it easier than ever to use
- To join, visit **Register.ConsumerSentinel.gov**

Consumer Sentinel is a secure online database of millions of consumer complaints available only to law enforcement. Complaints in Consumer Sentinel are about:

- Identity Theft
- Do-Not-Call Registry Violations
- Computers, the Internet, and Online Auctions
- Telemarketing Scams
- Advance-fee Loans and Credit Scams
- Sweepstakes, Lotteries, and Prizes
- Business Opportunities and Work-at-Home Schemes
- Health and Weight Loss Products
- NOW AVAILABLE: All consumer complaints filed with the FTC about financial issues, such as credit reports, debt collection, financial institutions, and lending.

Consumer Sentinel now offers you new and improved features.

- Find complaints more easily, with a tool that works like an Internet search engine
- Search within your search results
- Save data in your own 100 megabyte online storage center

Consumer Sentinel is a valuable resource.

- Search complaints from the FTC, the U.S. Postal Inspection Service, the Better Business Bureau, Canada's PhoneBusters, the Identity Theft Assistance Center, Internet Crime Complaint Center, and the National Fraud Information Center

Consumer Sentinel gives you the tools to investigate activity across jurisdictions.

- Find complaints from around the world – or around the corner – so you can do your job more efficiently and effectively

Consumer Sentinel enhances investigations.

- Get alerts about particular subjects or practices
- Find law enforcement agencies investigating the same targets
- Set up a search to run periodically

Consumer Sentinel is FREE.

- Your organization must sign a confidentiality and data security agreement with the FTC to access the updated Sentinel. Each user must register and obtain a user ID, a password, and a security token

To join, visit **Register.ConsumerSentinel.gov**

Somehow, your name and contact information ended up on a list created by somebody who passed it to several other somebodies, and now you're flooded with solicitations for all kinds of things you neither asked for nor wanted. What's a consumer to do?

You may not be able to get your name off all marketing lists, but there are ways to reduce the amount of unsolicited mail you receive.

To learn more:

For assistance on a wide range of consumer issues, contact the Department of Consumer Affairs' Consumer Information Center at 800.952.5210.

State of California
Department of Consumer Affairs

1625 North Market Blvd.
Suite N-112
Sacramento, CA 95834

800.952.5210 toll-free
800.326.2297 TDD

www.dca.gov

TAKE CHARGE! CALIFORNIA

dca

PDE 10_029 | 4.10

Can the trash talk!

How to cut down or stop unwanted phone, fax, mail, or e-mail ads

Regular mail

To stop most advertising mail:

The Direct Marketing Association's DMA Choice program allows you to request that specific companies or types of companies stop sending you unsolicited mail. It will take about 90 days for your preferences to take effect. The Direct Marketing Association represents most, but not all, direct marketers. Go to **www.dmachoice.org** to submit your request online. You can also make your request in writing. Send your letter to Mail Preference Service, Direct Marketing Association, P.O. Box 643, Carmel, NY 10512. Enclose a check for $1 made out to Direct Marketing Association. Do not send cash.

To stop credit card or loan offers:

A call to (888) 5OPTOUT or 888.567.8688 will stop most pre-approved credit offers from landing in your mailbox. You can choose to have your request stand for five years or permanently. Visit **www.optoutprescreen.com** to file the request online.

To stop catalogs:

Call the number on the specific catalog you are receiving, or send a letter requesting removal of your name and address (include the address label from the catalog). You can also register your request to stop specific catalogs online at **www.catalogchoice.org**. Not all catalogs are listed on the Web site.

Text messages

Report it:

State and Federal laws prohibit sending unsolicited text advertising to wireless devices such as cell phones and pagers. If you receive such messages, you can contact your wireless service provider or complain to the Federal Communications Commission at (888) TELL-FCC or 888.835.5322 or online at **www.FCC.gov**.

E-mail

Block it:

The use of an effective e-mail filter is the best way to block unsolicited e-mail. The most popular e-mail service providers offer filters. Check with your e-mail service provider for details.

Contact the senders:

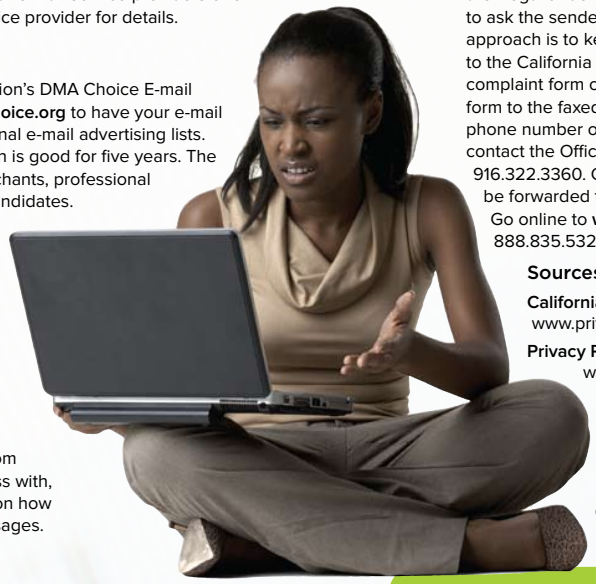
Find the Direct Marketing Association's DMA Choice E-mail Preference Service at **www.dmachoice.org** to have your e-mail address removed from some national e-mail advertising lists. Registration with eMPS Registration is good for five years. The request will not apply to local merchants, professional and alumni groups, and political candidates.

Report violators:

State and Federal laws forbid individuals and companies from sending commercial e-mail in many instances. Violators can be reported to the Federal Trade Commission at **spam@uce.gov.**

Exercise your opt out rights:

If you receive unsolicited e-mail from a company you have done business with, look for information on the e-mail on how to unsubscribe or stop future messages.



Phone calls

Register your phone number:

You can register your home and cell phone numbers with the National Do Not Call Registry, which was created by the Federal Trade Commission. Go online to **www.DoNotCall.gov** or call 888.382.1222 to register. The registration is permanent unless you remove it. It may take three months for your request to take effect. If you're not sure if you've registered your phone numbers, call or go online to verify. Remember, political solicitations, charities, and surveys are not covered by the registry, but if you tell them not to call you again, they have to honor your request.

Faxes

Keep and report:

Unsolicited ads sent by fax offering property, goods, or services are illegal under State and Federal law. Do not respond, even to ask the sender to stop sending the notices. Your best approach is to keep the fax and forward it with your complaint to the California Office of the Attorney General. Find the complaint form online at **www.ag.ca.gov**. Attach the complaint form to the faxed ads, and mail or fax them to the address or phone number on the form. For more information, you can contact the Office of the Attorney General at 800.952.5225 or 916.322.3360. Complaints about unsolicited faxes may also be forwarded to the Federal Communications Commission. Go online to **www.FCC.gov** or call (888) TELL-FCC or 888.835.5322 for information on how file a complaint.

Sources:

California Office of Privacy Protection
www.privacy.ca.gov

Privacy Rights Clearinghouse
www.privacyrights.org

Federal Trade Commission
www.ftc.gov

Federal Communications Commission
www.FCC.gov

The bottom line

Many unsolicited letters and e-mails are advertisements for legitimate products and services, but others are scams. Bogus stock tips, real estate investments, and foreign lotteries are some of the scams that may be sent via fax, mail, or e-mail.

Consumer Protection Division, Maryland Attorney General's Office Issue # 120

What's Your Consumer IQ?

Take this quiz to see how much you know about consumer issues, laws and scams

1. The only time you can get a copy of your credit report is when you apply for a loan or a mortgage. **True or False?**

2. After you sign a contract, including a contract to buy a car, you have three days to cancel if you change your mind. **True or False?**

3. You receive an e-mail that says your bank is updating its security measures and your account will be frozen unless you verify your account information. You should:

a) Give the information immediately.
b) Check that your bank's logo appears in the e-mail message; if it does, give the information.
c) Call your bank and ask if the e-mail is legitimate.

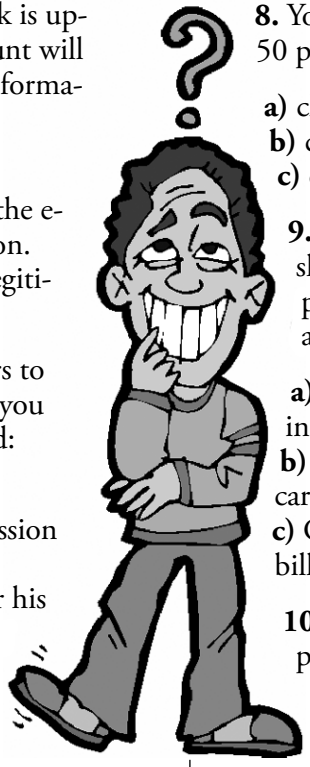
4. You should only hire licensed contractors to do repair work on your home. This means you should check that the contractor has a valid:

a) Commercial driver's license
b) Maryland Home Improvement Commission license
c) License from the national association for his professional specialty (electrician, plumber, etc.)

5. Your credit card says it has a "universal default" policy. This means that:

a) If you make a payment late to another creditor, it will raise your interest rate.
b) It offers accident insurance when you rent a car.
c) If you default on your payments, it will close your account.

6. By law, all pharmacies must charge the same price for a prescription drug. **True or False?**



7. You agree to co-sign a car loan for your younger brother. If he defaults, can you be held responsible for any of the debt?

a) No, as a co-signer you are only acting as a reference.
b) Yes, for 50 percent of the debt.
c) Yes, for 100 percent of the debt.

8. You are ordering furniture and the store requires a 50 percent deposit. What is the safest way to pay?

a) check
b) credit card
c) cash or debit card

9. You recently had surgery. You received statements showing that the surgeon and the hospital were paid by your insurance plan, but then you receive a bill from a laboratory. You should:

a) Assume the lab tests are not covered by your insurance and pay the bill.
b) Don't do anything, the insurance plan will take care of it.
c) Call your insurance plan to find out why the lab bill wasn't paid.

10. What is the surest sign that a work-at-home opportunity is a scam?

a) It gives a post office box as an address.
b) It requires you to send money in advance for supplies or instructional materials.
c) It advertises on telephone poles.

11. A landlord can keep your security deposit after you move out:

a) For routine painting and carpeting
b) If he sends you a list of damages you caused and what it actually cost to repair them
c) If he says your pet made the carpets smell

ANSWERS

1. False. You can order a copy of your credit report at any time. In fact, it's a good idea to review your credit report annually, to catch mistakes or to spot signs that someone is using your data to commit identity theft. By law, you have the right to a free copy of your credit report annually from each of the major credit reporting companies. Call 877-322-8228 or visit www.annualcreditreport.com.

2. False. There are a few transactions for which the law allows a cancellation period (such as a door-to-sales or health club contract), but most contracts are binding when you sign them. The often-repeated myth that you can cancel a signed contract has given many consumers a false sense of security when making an expensive purchasing decision, like buying a new car.

3. c. Call the bank at the number listed in the phone book. Banks do not ask their customers to verify sensitive information by e-mail. Con artists send these messages to try to steal your identity and use it to make fraudulent withdrawals or credit applications. Their phony e-mails can look very authentic.

4. b. Home improvement contractors are required to be licensed by the Maryland Home Improvement Commission. Be sure to check that a contractor you are considering using has a current license. Call the Commission at 410-230-6309. If a licensed contractor fails to do the job, or does it poorly, you may be able to recover your losses through the Home Improvement Commission's Guaranty Fund.

5. a. Many credit cards have a "universal default" policy. They monitor your credit file. If you are late paying any creditor, they consider that you are a higher credit risk and they will raise your rate.

6. False. Pharmacies can charge different prices for prescription drugs.

7. c. The bank can hold you responsible for 100% of the amount owed.

8. b. It's safer to use a credit card when paying in advance for an item. If the store should go out of business or something similar happen before you get your furniture, you might be able to get a "chargeback" from your credit card. If you paid by check, cash or debit, you might never get the money back.

9. c. Call your insurance plan. If you need further help with a medical billing or health care question or dispute, you should call the Attorney General's Health Education and Advocacy Unit at 410-528-1840.

10. b. If a company requires you to pay money up front, beware. It's against state law for a company that advertises a work-at-home opportunity to require advance payments for materials. You'll probably receive worthless materials and find that there's no way to make money.

11. b. If the landlord withholds any part of your security deposit, he or she must send a list of damages you caused and what it actually cost to repair them within 45 days after you move out.

How did you do? You can find information about many other consumer issues at the Attorney General's website at www.oag.state.md.us/Consumer.

Attorney General's Consumer Offices

Consumer Protection Division
200 St. Paul Place, 16th Fl.
Baltimore, MD 21202-2021

- General Consumer Complaints: 410-528-8662
  Toll-free: 1-888-743-0023
  TDD: 410-576-6372
  9 a.m. to 3 p.m. Monday-Friday
- Medical Billing Complaints: 410-528-1840
  9 a.m. to 4:30 p.m. Monday-Friday
  To appeal health plan claims decisions:
  Toll-free within Maryland 1-877-261-8807

Branch Offices

- **Cumberland**
  301-722-2000; 9 a.m. to 12:00 p.m. 3rd Tuesdays
- **Frederick**
  301-600-1071; 9 a.m. to 1:00 p.m. 2nd and 4th Thursdays
- **Hagerstown**
  301-791-4780; 8:30 a.m. to 4:30 p.m. Monday-Friday
- **Prince George's**
  301-386-6200; 9:00 a.m. to 5:00p.m. Monday-Friday
- **Salisbury**
  410-713-3620; 8:30 a.m. to 4:30 p.m. Monday-Friday
- **Southern Maryland (Hughesville)**
  301-274-4620 Toll-free 1-866-366-8343
  9:30 a.m. to 2:30 p.m. Tuesdays

The Consumer's Edge is produced by the Maryland Attorney General's Office. Reprints are encouraged. Free subscriptions are available to groups wishing to distribute to their members. Call 410-576-6578.

www.dsef.org • T: 202.452.8866