Federal Trade Commission

Remarks of FTC Chairman Deborah Platt Majoras[1]
AARP National Event & Expo: Life@50+
September 6, 2007
Boston, Massachusetts

"Protect Your Identity, Yourself and Your Family: A Conversation with Federal Trade Commission Chairman Deborah Platt Majoras"

I. Introduction

Thank you, Robin. I am delighted to be here this afternoon. The AARP has been a tremendous partner to the Federal Trade Commission (FTC), as together we have worked to battle fraud and educate consumers. The FTC works for you – the consumer – and so it is important not only that I have the opportunity to describe what we are doing and how it benefits you and your families, but also that I hear your concerns.

The marketplace issues that are on the minds of consumers are wide-ranging and ever-changing. At the forefront today are such issues as identity theft, spam, false claims for health care products, and financial scams. While these topics are widely-covered in the news, I intend to go beyond the headlines to give you a better understanding of what the FTC is doing about these problems and, even more importantly, what you, as a consumer, can do about them.

II. What is the FTC?

To provide some context, the FTC is a relatively small law enforcement agency with 1,000 lawyers, economists, outreach specialists, and support staff. We have five Commissioners,

[1] These remarks are my own and do not necessarily represent the views of the Commission or any other Commissioner.

each appointed by the President and confirmed by the Senate. Despite our small size, the FTC has a very broad mandate: we are the nation's primary consumer protection agency, and we are charged with protecting competition through enforcement of the nation's antitrust laws. When businesses compete fairly within a set of rules, consumers win. When the market is open and free, legitimate businesses compete on the merits, and consumers have access to quality goods and services and lower prices. But, of course, not all businesses are legitimate, and even some that are want to cut corners and exaggerate (or worse) in making claims about their products. As a consumer, you need truthful information to help you make purchasing decisions. So, in addition to working to ensure a competitive marketplace, we seek out and challenge unfair and deceptive practices in the marketplace.

The FTC's work directly impacts you as a consumer. You might wonder where you should go for help if you become a victim of identity theft. You might wonder whether that pill advertised on TV late at night could possibly cause all that weight loss. You might worry that a merger of two pharmacies in your neighborhood might mean higher prices and less choice. In each of these situations, the FTC works to protect you and help you protect yourself.

III. Identity Theft

In the past few weeks, the FTC has received consumer complaints that have included the following:

- A woman from Massachusetts called to report that an identity thief had obtained a $100,000 business loan in her name.
- A man from Connecticut reported that an identity thief created a fake driver's license and obtained a power of attorney in his name, and then secured a mortgage for over $400,000.
- Another consumer discovered that his identity had been stolen when the IRS tried to collect a debt from him after a fraudulent tax return had been submitted in his name.

> This consumer ultimately learned that the identity thief had opened over ten credit card accounts in his name and obtained a new mortgage for over $300,000. He has spent countless hours closing these accounts and correcting these problems.

Unfortunately, these complaints are not atypical. Identity theft afflicts millions of Americans, costing consumers and businesses valuable time and precious dollars. We hear from 15,000 to 20,000 consumers each week, many with similar stories, of the financial toll on victims and the time that they spend recovering their identity. This does not begin to address the emotional toll of the identity theft, which is impossible to quantify.

Congress has assigned the FTC a unique role in combating identity theft and coordinating government efforts,[2] and we devote significant resources to protecting you from identity theft and to helping you if you do become a victim. We take consumer complaints, which then are added to our Identity Theft Data Clearinghouse, a centralized database used by over 1,500 law enforcement agencies; we assist victims and consumers by providing information and education; we educate businesses on sound security practices and prosecute those whose efforts fall short; and we train local law enforcers, the first responders in identity theft cases. In addition, I co-chair the President's Identity Theft Task Force, which coordinates the federal government's efforts to combat identity theft.

The first step in preventing identity theft is safeguarding personal information. There are steps that you can take, but we recognize that you also need to rely on others, namely government agencies and businesses, to safeguard the sensitive information that they get from you. Governments need to collect personal information from you to provide you with certain services – from drivers' licenses to social security and medicare benefits to tax refunds. Businesses also have important information about you – restaurants and stores have your credit

[2] In 1998, Congress passed the Identity Theft Assumption and Deterrence Act ("the Identity Theft Act"), Pub. L. No . 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

card numbers, banks have your account numbers, mortgage companies have your credit reports, and insurance companies have your medical information. A disgruntled employee, an unscrupulous hacker, or a plain-old thief can intercept this information, impersonate you, and run up hundreds of thousands of dollars in your name.

As a federal government agency, we are implementing recommendations of the President's Identity Theft Task Force aimed at improving the security of the data we collect from you. We are improving internal data security processes; reducing unnecessary uses of Social Security numbers, which are often the key item of information that identity thieves need; and developing plans for responding in the event of a breach, including notification to affected persons.

We also are ensuring that the private sector maintains reasonable security for your personal information. The FTC has brought 14 actions against businesses for their failure to provide reasonable security for consumer data. Those we have prosecuted include retailers, such as BJ's Wholesale Club and DSW Shoe Warehouse; information services, such as ChoicePoint; and data processors such as CardSystems Solutions.[3] In one case, the FTC alleged that a company threw files containing consumer home loan applications into an unsecured dumpster. In other cases, we found that retailers stored sensitive information in multiple files when there was no longer a business need to keep the information. Or they stored information in unencrypted files that could be easily accessed using commonly-known user IDs and passwords such as – you guessed it – "password." In yet other cases, companies failed to implement

[3] *See* FTC Press Release, *BJ's Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards* (June 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.shtm;FTC Press Release, *DSW Inc. Settles FTC Charges: Agency Says Company Failed to Protect Sensitive Customer Data* (Dec. 1, 2005), *available at* http://www.ftc.gov/opa/2005/12/dsw.shtm;FTC Press Release, *Choicepoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm;FTC Press Release, *CardSystems Solutions Settles FTC Charges* (Feb. 23, 2006), *available at* http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm.

simple, low-cost, and readily available defenses to well-known Web-based hacker attacks or failed to use readily available security measures to prevent unauthorized wireless connections to their networks. In perhaps our most well-known data security case against the information broker Choicepoint, we alleged that the company sold sensitive consumer information to identity thieves posing as the company's clients, despite the clear warning signs of fraud.

No doubt you continue to read about data security breaches in the news. Be assured that the FTC continues to monitor the marketplace and, in appropriate cases, will bring enforcement action. We have several investigations underway.

We also continue to seek to educate businesses and consumers about identity theft. For businesses, the message is to protect their customers' information. It's good business, and it's the law. This spring, we unveiled a new business education guide on data security.[4] The Commission anticipates that the brochure will prove to be a useful tool in alerting businesses to the importance of data security issues and giving them a solid foundation on how to address them.

We will continue to hold our government and the business community to high standards for data security. But you, too, have an important role to play. Last year, we launched a nationwide identity theft education program urging consumers to deter, detect, and defend against identity theft.[5] To ensure that the Deter, Detect, Defend campaign is effective, we created a consumer education kit that all organizations can use to educate their employees, their customers, and their communities about how to minimize their risk. The kit includes a victim recovery guide, a training booklet, a guide to talking about identity theft, presentation slides, an easy-to-read brochure, and a 10-minute video. We have distributed more than 2.6 million brochures and 55,000 kits to date – we even have some at our booth in the Exhibit Hall. And we

---

[4] *Available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html.

[5] *See* FTC Press Release, *FTC Launches Nationwide Id Theft Education Campaign* (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/ddd.htm.

have formed many partnerships to help us broaden our reach – including with AARP, where state offices have used the kit to train Fraud Fighters to go into the community and educate.

Let me offer some practical advice from our campaign. To **deter** ID theft, start with protecting your Social Security Number. Leave your Social Security card in a safe place at home, rather than carrying it with you. The same goes for Medicare cards or any other card with your Social Security Number. Bring them with you if you need them, but otherwise, leave them safely at home.

Be careful about your mail and trash. ID thieves still use low-tech ways to get personal information, so you can make it harder for them by shredding bills or statements before throwing them away. You can reduce the chances that your mail will be stolen by using a locking mailbox, and by stopping your mail when you go on vacation. And you can consider opting out of pre-screened credit offers, which would reduce the amount of mail you get. You also should keep important financial documents in a safe place at home, away from prying eyes. And, if you no longer need a financial document, it is best to shred it.

Use strong passwords when you go online. These are passwords that combine letters, numbers and symbols, and are never words – even words spelled backwards – or important dates, like birthdays or anniversaries. To make them easy for you to remember, you can substitute numbers or symbols for letters – using a dollar sign for an "S", or a "3" instead of an "E". You can also think of a phrase and use the first letters: for example, "the Cleveland Browns win the Superbowl" becomes "T-C-B-W-T-S." (Believe me, I have been waiting my whole life for that to happen – no identity thief would come up with that one!) These tricks make it harder for ID thieves to get to your sensitive information.

You can **detect** identity theft in two key ways. First, read your bills and statements carefully. If an ID thief has obtained access to your bank account or credit card, activity should show up on your statements. The sooner you spot the theft, the sooner you'll be able to address

it and stop the thief. Second, check your credit report. This is a good way to make sure that no one but you has opened any new accounts in your name. It is your right to get one free copy of your report from each of the three nationwide credit reporting companies each year. You can do this by visiting annualcreditreport.com, which is the *only* source of the free annual credit reports.

If your identity is stolen, you can **defend** your good name by taking four steps immediately:

1. Call one of the three credit reporting companies to report the ID theft and place a fraud alert;
2. Close any accounts that have been affected;
3. File a report with law enforcement; and
4. File a complaint with the FTC at ftc.gov/idtheft.

Filing a complaint with the FTC serves two key purposes. First, complaints are vital to the FTC's work. Each complaint filed with us goes into a database that law enforcement can use in their investigations. The complaints help us find patterns and similar crimes, and help law enforcers in different jurisdictions make their cases. Second, filing a complaint can help you vindicate your legal rights. For example, our counselors can use the information provided by the victim to fill out an identity theft report, which the victim can take to a local police station and then use it to have fraudulent accounts removed from his or her credit report.

If you or someone you know is a victim of identity theft, in addition to following these tips, I would urge you to read our recently-released "Identity Theft Victims Statement of Rights," which you can find on our website. The Statement outlines your rights when dealing with credit reporting agencies, law enforcement agencies, creditors, debt collectors, and others. To make the recovery process easier for victims of identity theft, we are also working to educate law enforcement on the importance of taking reports. And we are working with the credit reporting companies to try to make consumer interactions with them more productive.

IV. Spam

Email technology has brought us great gifts in the form of quick and efficient communication. Email makes it easier to stay in touch with old friends, children, and grandchildren, and it allows many of us to work remotely. But it also has brought us spam, which has the potential to inundate our in-boxes with unwanted email, facilitate fraud, and undermine our trust and confidence in the Internet.

The volume of unsolicited emails being reported by email filtering companies is rising, increasing costs for businesses and consumers alike. Even more troubling, spam reaching consumers' inboxes is more often being used to launch phishing attacks and to deliver malicious code or "malware" to consumers' computers. This new generation of malicious spam goes beyond mere annoyance – it can result in significant harm to consumers and undermine the stability of the Internet and email in particular.

The FTC is working to combat malicious spam in several ways. The first is through law enforcement. We cannot permit the electronic world to become a lawless frontier. Since 1997, the Commission has aggressively pursued deceptive and unfair practices perpetrated through spam in 90 law enforcement actions against 143 individuals and 100 different companies, with 26 of the cases brought after Congress enacted spam legislation known as the CAN-SPAM Act.

For example, the FTC has brought several cases challenging spammers' failure to inform recipients that email contains sexually explicit content. The FTC's Adult Labeling Rule and the CAN-SPAM Act require commercial e-mailers of sexually explicit material to use the phrase "SEXUALLY EXPLICIT" in the subject line, and to ensure that the initially viewable area of the message does not contain graphic sexual images.[6] In 2005, the FTC sued seven companies in a crackdown on illegal "X-rated" spam that violated CAN SPAM and the Adult Labeling Rule.

---

[6] *See* FTC Press Release, *FTC Adopts Rule That Requires Notice That Spam Contains Sexually-Explicit Material* (Apr. 13, 2004), *available at* http://www.ftc.gov/opa/2004/04/adultlabel.shtm.

Since then, the FTC has settled with five of the companies and obtained civil penalties against them totaling $1.6 million.[7]

Although spam frequently is associated with adult content, it also commonly is used to hawk a range of bogus products and services. And, the FTC aggressively challenges these other forms of spam also. Just a few weeks ago, the FTC stopped a spam operation that inundated consumers with emails linking to websites where marketers made false claims that a pill could increase human growth hormone (HGH) levels in the body and as a result reverse the effects of aging.[8] The litigation is still ongoing, and we will be seeking strong remedies against the spammers.

While the cases we have brought to date have been significant, we recognize, of course, that we cannot battle this pernicious problem alone. This summer, we hosted a Spam Summit to learn more about malicious spam and discuss new approaches to fighting it. The Summit panelists, nearly 50 in number, all confirmed that spam is being used increasingly as a vehicle for more pernicious conduct that is often criminal in nature. Thus, we affirmed that we need to continue to build partnerships with criminal law enforcement agencies such as the Department of Justice to fight spam.

We also confirmed the need for government agencies to work with the private sector. Malicious spam is a technological problem, driven largely by botnets and the exploitation of computer security vulnerabilities that allow spammers to operate anonymously. Industry is taking a leading role in developing technological tools, such as domain-level email

---

[7] *See* FTC Press Release, *FTC Cracks down on Illegal "X-rated" Spam* (Jul. 20, 2005), *available at* http://www.ftc.gov/opa/2005/07/alrsweep.shtm. *See also* FTC Press Release, *Adult Entertainment Marketer Settles FTC Charges* (Jan. 30, 2007), *available at* http://www.ftc.gov/opa/2007/01/tjweb.shtm.

[8] *See* FTC Press Release, *FTC Stops Spammers Selling Bogus Hoodia Weight-Loss Products and Human Growth Hormone Anti-Aging Products* (Aug. 23, 2007), *available at* http://www.ftc.gov/opa/2007/08/hoodia.shtm.

authentication, to "uncloak" these anonymous spammers, and the Commission is encouraged by reported increases in the adoption rates for email authentication.

We also are working more closely than ever with our international counterparts to share information and cooperate on investigations to bring spammers to justice, no matter where in the world they are located. Just last year, Congress gave us new tools to fight any kind of fraud that crosses international borders, and we are beginning to use these new tools so that we can be more effective in combating cross-border fraud.

Of course, another key component of combating spam is educating consumers. Because spam costs virtually nothing to send, even if only one in a million consumers responds by sending money or personal information in response to a spam email, it is worth it for spammers to send. Our message to you is: Don't let this happen; when you receive spam, hit the delete button.

The centerpiece of our efforts to educate consumers about spam is OnGuardOnline.[9] OnGuardOnline.gov is an innovative multimedia website developed in partnership with other government agencies and the technology industry. It provides general information on online safety, interactive educational games that teach consumers how to spot online scams, and specific information on a range of topics. Since its launch in late 2005, OnGuardOnline has attracted more than 3.5 million visits.

One of the "modules" on our OnGuardOnline site is devoted to a particular type of spam called "phishing," spelled with a "p-h." By now, we all likely have received those emails that purport to come from banks or other legitimate businesses and look remarkably real, but ask us to "confirm" our account number or Social Security Number or our account will be shut down.

---

[9] *See* FTC Press Release, *FTC and Partners Urge Consumers to Be OnGuard Online* (Sept. 27, 2005), *available at* http://www.ftc.gov/opa/2005/09/onguardonline.htm.

For example, you might get an email from someone posing as an officer of the Social Security Administration asking you to send your Social Security Number to confirm your benefits. Or, you might get an email from the IRS asking for financial information to process your tax refund. This is phishing.

Our education message to consumers is simple: never give your personal information to anyone who contacts *you* – whether it is through email, telephone, or in person. If you receive one of these emails asking for account numbers, don't reply, and don't click on the link in the email. Legitimate companies will never contact you by email or telephone to request your personal or financial information. If you are concerned about the account in question, contact the organization in question using a phone number or email address that you know to be correct. Never use a phone number or address given in the phishing email.

While this new generation of spam poses risks to your computer and your personal information, we should not ignore lower-tech attempts to separate consumers from their money. Every year, the FTC compiles its complaint statistics and issues a list of the top ten scams – and every year, **foreign money offers** make that list. These spam emails, sometimes known as "Nigerian letters," purportedly come from a foreign government official who politely promises big profits in exchange for help in moving large sums of money out of their country. They appeal to your compassion while trying to convince you to let them transfer millions of dollars into your bank account – and to give them money up front to cover "transaction costs," "lawyers fees," or "customs."

This particular scam has been around for decades, even before email made it easier and cheaper for scammers to reach consumers. But consumers can help stop this scam by doing just as they do with phishing emails: hitting delete. And, should you or anyone you know ever be tempted, ask yourself these questions: First, why would a perfect stranger pick you – also a

perfect stranger – with whom to share a fortune? And second, why would you share your personal or business information, including your bank account number, with someone you do not know? If it sounds too good to be true, that's because it is.

You can also forward any spam emails to the FTC's spam database at this address: spam@uce.gov. The FTC and its law enforcement partners use this database to generate cases against spammers. Once you send your spam to us, be sure to delete it from your own computer.

V. False Claims About Health Care Products

The FTC also has a vigorous enforcement program directed at deceptive advertising. Within this realm, a top priority is to prosecute companies that make bogus claims about health care products and, when possible, getting money back to consumers who were scammed. Too often, consumers fall prey to fraudulent health claims for pills, creams, and devices because they are desperate for help. Fifty million Americans suffer from a chronic pain condition[10] and have found no effective cure or treatment.[11] Seventy million Americans are trying to lose weight.[12] Millions more suffer from diseases such as cancer and diabetes. And, unfortunately, unscrupulous individuals are standing by to take advantage.

Take this claim, made in an infomercial. A woman suffering from ovarian cancer spoke of the insufferable pain she endured from multiple rounds of chemotherapy: "There's just some mornings I just can't even get out of bed," she says before describing how this particular product

---

[10] Source: American Chronic Pain Association, "Pain Fact Sheet," *available at* http://www.theacpa.org/pu_main_02.asp.

[11] Source: National Pain Foundation, "Key Messages About Chronic Pain," *available at* http://www.nationalpainfoundation.org/NationalPainAwareness/KeyMessagesAboutChronicPain.DOC

[12] Source: Journal of the American Medical Association, "Prevalence of Attempting Weight Loss and Strategies for Controlling Weight," *available at* http://jama.ama-assn.org/cgi/content/abstract/282/14/1353.

transformed her life, "I'm just amazed and in disbelief. I'm just excited that, you know, my life is normal again."[13]

The ad was for the Q-Ray bracelet. Andrew Park and his companies advertised the Q-Ray bracelet as a device for relief for all kinds of pain. Through infomercials, the Q-Ray defendants raked in net sales of *$87 million*, selling their bracelets at prices as high as $250, a mark-up of more than 650 percent. The court found the defendant companies and Mr. Park guilty of false and misleading advertising, both about the pain relief benefits of the bracelet and about the 30-day satisfaction guarantee promise of a full refund, and ordered them to pay up to $87 million in refunds to consumers – the entire net sales generated by the deceptive infomercials. This was a big victory for consumers and a strong deterrent for fraudulent marketers.

In another case, the FTC stopped marketers of a purported Chinese herbal remedy called "Dia-Cope" from making false claims that the supplement could prevent, treat, and cure diabetes.[14] We also alleged that the Dia-Cope marketers misrepresented that clinical trials proved their disease claims and that the FDA had approved their product. The FTC order against them bans future disease prevention, treatment, and cure claims and required that they give up all their ill-gotten gains.

For years, unscrupulous marketers also have exploited Americans' struggle to shed weight. In our country, 66% of the adult population is overweight, and thus it is not surprising that we have 70 million people trying to lose weight.[15] We are all too familiar with the pitches for miracle weight-loss products and potions, which are rampant in this country. Products like

---

[13] *FTC v. QT, Inc.*, 448 F. Supp.2d 908, 924-25 (N.D. Ill. 2006).

[14] *See* FTC Press Release, *Repeat Offenders Banned From Claiming Products Treat or Cure Diseases* (Aug. 10, 2006), *available at* http://www.ftc.gov/opa/2006/08/sagee.shtm

[15] *See* National Center For Health Statistics, "Prevalence of Overweight and Obesity Among Adults: United States 2003-2004," *available at* http://www.cdc.gov/nchs/products/pubs/pubd/hestats/overweight/overwght_adult_03.htm.

"Fat Trapper" and "Exercise in a Bottle" promise fast and easy weight loss with claims that you can "eat what you want and never – ever – ever have to diet again."[16] But wait, there's more! One marketer even promised that its product would work faster than a hunger strike! "Even if you eat nothing you won't slim down as fast," the ad promised, claiming the product would burn off "more fat than running 98 miles per week."[17] Earlier this year, we announced settlements with the makers of four significant and high-profile weight-control and weight-loss products, Trimspa, Cortislim, Xenadrine, and One-A-Day WeightSmart.[18] The marketers of the product Xenedrine agreed to pay at least $8 million and up to $12.8 million in consumer redress to settle FTC charges that they made false and unsubstantiated weight-loss claims. Ads for Xenadrine EFX promised rapid and substantial weight loss despite the fact that one of their studies showed more weight loss in the placebo group than in the group taking Xenadrine. The Xenadrine ads also featured testimonials from extremely trim and muscular consumers – who failed to mention not only that they had been paid up to $20,000 for their testimonials but also that their "After"-photo bodies were actually the product of rigorous diet and exercise programs.

As consumers, you can do your part, too. A healthy dose of skepticism is helpful when you consider these products. As you see ads for health-related products, watch for statements that the product is a cure-all for a wide variety of ailments, or that the product can treat or cure diseases. These are signs of a fraudulent claim. Some others are promotions that use words like "scientific breakthrough," "secret ingredient," or "ancient remedy;" undocumented case histories or personal testimonials by consumers or doctors claiming amazing results; limited availability

---

[16] These and other claims made in an infomercial for two dietary supplement products were challenged by the Commission as false and misleading. *See FTC v. Enforma Natural Prods., Inc.*, Civ. Action No. 04376JSL (CWx)(C.D. Cal. 2000)(stipulated final order).

[17] In the Commission's case against this marketer of the "Himalayan Diet Breakthrough" the FTC obtained an order requiring payment of $400,000 in consumer redress. *FTC v. AVS Marketing, Inc. et al.*, Civ. Action No. 04C-6915 (N.D. Ill. June 25, 2005).

[18] See FTC Press Release, Federal Trade Commission Reaches "New Year's *Resolutions with Four Major Weight-Control Pill Marketers* (Jan. 4, 2007), *available at* http://www.ftc.gov/opa/2007/01/weightloss.htm.

and advance payment requirements; and promises of no-risk money-back guarantees. Watching for these warning signs can help keep you from being taken in by fraud.

VI. Financial Issues

Another group of consumers who are vulnerable to fraud are those with credit or debt problems. Unfortunately, many consumers with financial problems have fallen prey to deceptive debt negotiation or other credit repair schemes. You may have seen advertisements, or even received fliers or telemarketing calls, about companies that offer to fix your credit. They claim to erase bad credit, create a new credit identity – legally (which, by the way, is not possible – legally), and remove bankruptcies, bad loans, and liens from your credit file.

Since 2003, the Commission has brought about a dozen cases challenging these type of financial practices, obtaining orders for redress or civil penalties of more than $40 million. We have challenged, for example, those offering debt reduction services that charge hidden fees, those that promise to lower consumers' debts, and even those that claim they can eliminate accurate negative information from consumers' credit reports.

Of course, legitimate credit counseling organizations can provide valuable services to consumers, and we encourage consumers to use them. But, there is, of course, no magic bullet to repairing bad credit. Only time, a conscious effort, and a personal debt repayment plan will improve your credit record. You can spot the warning signs of credit deception, starting with those too-good-to-be-true claims. Other signs to look for are companies that want you to pay for credit repair services before they actually provide any services; companies that do not tell you your legal rights or what you can do yourself for free; companies that recommend that you not contact a credit reporting company directly; and companies that suggest that you try to invent a "new" credit identity.

Another issue facing some people in financial difficulty is abusive **debt collection**. As consumer debt levels have risen, so have complaints to the Commission about debt collectors. We receive more complaints about debt collectors than any other single industry, with more than 69,000 complaints about third-party debt collectors in 2006.

In one recorded call to a young woman, for example, a debt collector said: "You think you're so special, you're going to see how special you are when we back a moving truck up to your front door and load up everything you thought you ever owned . . . and hold an auction to pay your debt . . . As far as I'm concerned you and him [her father] are both a couple of liars . . . Little girl, shut up, you don't know anything, okay?"

We sued to stop that debt collector's repeated violations of the law. The Commission alleged that the debt collector, Rawlins & Rivera, engaged in deceptive and abusive debt collection practices, including making false threats that consumers will face immediate suit, property seizure, wage garnishment and even arrest if they do not immediately pay their debts.[19] We also alleged that the defendants often embellished their empty threats with abusive and profane language, as well as threats to reveal the debt to relatives and others. They even used these same practices in an attempt to collect debt from relatives. We have asked the court to immediately stop these practices and to order the defendant to disgorge their ill-gotten gains. We succeeded in stopping the practices, and the litigation is ongoing.[20]

When it comes to credit and debt issues, we want consumers to know their rights and obligations. Our website, ftc.gov, provides information that can help consumers learn about their rights and what they can do if those rights are violated. Often, one step is filing a complaint

---

[19] *See* FTC Press Release, *FTC Asks Court to Stop Abusive Debt Collectors* (Feb. 2, 2007), *available at* http://www.ftc.gov/opa/2007/02/rri.htm.

[20] We continue to monitor the practices of the debt collection industry. This October, we will host a workshop to examine changes in the debt collection industry and the related consumer protection issues. *See* FTC Press Release, *FTC Asks Court to Stop Abusive Debt Collectors* (Feb. 2, 2007), *available at* http://www.ftc.gov/opa/2007/02/rri.htm.

with the Federal Trade Commission. Although we do not have the staff to investigate every complaint individually, your complaint, combined with those of other consumers, add up to cases that can be brought to help protect all consumers. And out of those cases comes yet more consumer education as we learn about new scams or ways bad actors are using to defraud you. We work hard at the FTC to stay a step ahead of the scammers. All of you can help us by reporting fraud when it happens to you.

VII. Conclusion

I appreciate the chance to talk with you today about what the FTC does for consumers, what you can do to protect yourself and your family from some common scams, and how you can help other consumers – and the FTC – by reporting fraud. I hope that you will visit our booth in the Exhibit Hall – booth number 1169 – where we have materials and staff who can answer questions we don't get to here. There are also materials in the back of the room, so please take some.

As we close, I would like to leave you with just a few general tips on being a savvy consumer:

- Protect your personal information: share it only with those you know and trust.
- Take your time: resist any offers to "act now".
- Read the small print: get promises in writing, read the paperwork before signing any thing or making any payments, and pay special attention to the small print.
- Shop around: Compare prices and features to make sure you are taking advantage of the benefits free competition has to offer.
- Trust your instinct – If it sounds too good to be true, that is because it is.
- Report fraud. If you think you've been the victim of fraud, report it at ftc.gov.

Thank you for being here. I am happy to take your questions.