

28

HOW TO AVOID MAIL ORDER AND TELEPHONE FRAUD

§ 28. 1. Introduction

This consumer rights chapter provides information on your rights when you suspect the possibility of mail order or telephone fraud. It contains the following sections:

- § 28. 2. A Billion Dollar Problem
- § 28. 3. How To Spot Mail, Telephone or Internet Fraud
- § 28. 4. How To Avoid Becoming A Victim
- § 28. 5. Examples Of Telemarketing Fraud
- § 28. 6. Credit Card Purchases
- § 28. 7. C.O.D. Purchases
- § 28. 8. Pay-Per-Call
- § 28. 9. Automatic Checking Account Debit Scams
- § 28. 10. Protect Against Fraudulent Telemarketers
- § 28. 11. Slamming and Cramming
- § 28. 12. Identity Theft
- § 28. 13. "Do Not Call" List (And Do Not Mail)
- § 28. 14. Agencies Which Can Help You
- § 28. 15. E-Mail Spam

§ 28. 2. A Billion Dollar Problem

Fraudulent telemarketers and mail order swindlers will steal a billion dollars or more this year from American consumers. These professional con artists peddle everything from over-priced and ineffective water "purifiers" to "gold mines" that are nothing more than piles of dirt.

These scam artists are very inventive and persuasive. Telephone calls and colorful mailings offering products at greatly reduced rates, "free prizes" or large sums of cash if you buy can sound very exciting. But they simply are lies.

Of course, selling products or services by phone or by mail is not in itself a crime. Most mail order or telemarketing companies represent honest, reputable businesses. But because so many customers enjoy the ease and convenience of buying by phone or by mail, it is an attractive tool for unscrupulous salespersons.

In our opinion, if you receive a mail order or telephone solicitation that seems to provide an extremely attractive product at very little cost, *you should ignore it*. If it sounds too good to be true, then without a doubt, it is not true. How can we say this with such confidence? Very simply: no business can survive if it gives away free prizes or charges very little for such prizes. The salesperson will make clever claims—*e.g.*, your prize is part of a national promotion that will bring them even more customers¹—but they will be lies. *If to win a prize you have to pay the caller any amount of money—hang up! It's undoubtedly a scam!*

Most recently, telephone callers are pursuing a new fraud: “stealing” your identity so they can make unauthorized changes against your accounts. *See* § 28.12 on how to protect yourself.

The Federal Trade Commission, the State Attorneys General, the Better Business Bureau, and others are working hard to put fraudulent mail and telephone solicitors out of business. Over the last several years, the FTC has closed down telemarketing scams with sales of more than \$780 million. And in the past two years, the Attorneys General have taken action against 150 operations.

Unfortunately, though, fraudulent mail and telephone solicitors are very hard to track down. Most are “fly-by-night” operations working out of so-called “boiler rooms”—leased space with banks of telephones staffed by professional scam artists. Once under investigation, these boiler rooms can easily shut down and move—virtually overnight—to another town, state or country. They may even change their name—anything to cover their tracks.

Maine consumers are protected by several laws that make it both a crime and an unfair trade practice to commit telephone or mail fraud. These laws are discussed below. But our penalties are very hard to enforce. Telemarketers never locate in the states in which they place their phone calls and our local police can do little when Mainers complain.

Because enforcement is so difficult, it is essential that today's consumer be an informed mail order and telephone shopper. The following tips suggest how you can detect mail and telephone fraud and avoid becoming a victim.

Please note: Federal and State law² allows you to inform a telemarketer who calls you that you do not want to be called again. The telemarketer must take note of this and remove your name from its call list. Take notes on any telemarketer who you tell to stop calling. If they call again you may be able to collect up to \$500.³ *See* § 28.13 for information on how to put your name on the “Do Not Call” List maintained by the Federal Trade Commission and the Maine Attorney General.

¹ The Maine Attorney General brought an unfair trade practice action against Capital Advertising, a telemarketer that moved into Maine in the spring of 1992. Here is one of the many telephone scripts Capital Advertising used to get consumers to send the \$649 for a “gift pack” and one of 5 guaranteed prizes:

HOW CAN WE AFFORD TO GIVE OUT MAJOR AWARDS? [Name of Consumer], the best way I can make sense of this is to explain it this way. Let's say you get the \$5,000.00 cashier's check, a picture of you and your award in my catalog will bring me a hundred new customers who spend an average of a thousand dollars each, that's 100,000 dollars. Then it's well worth my effort to give you one of these five awards, I only ask two things, enjoy the award and give me your word that I'll get a good clear picture for my catalog. FAIR ENOUGH?

In fact, no matter what the consumer received, if anything, it was worth *far less* than the \$649 price. Yet, many consumers fell for such trickery. *See State v. Capital Advertising, Inc. et al.*, (Me. Super. Ct., Kenn. Cty., August 18, 1992). As a result of our lawsuit, consumers received back approximately \$200,000.

² The Telephone Consumer Protection Act also bans junk faxes and recorded calls.

³ 47 U.S.C. § 227(c)(5), 10 M.R.S.A. § 1499.

§ 28. 3. How To Spot Mail, Telephone or Internet Fraud

There are many kinds of mail, telemarketing and internet scams, and new ones are invented every day. But certain elements are common to most of these scams. BEWARE OF:

- A. “Free gifts” that require you to pay shipping and handling charges, “redemption” fees, or require you to phone a 900 or 809 number in order to take advantage of the attractive offer. These are “pay per call” lines and you risk getting billed an outrageous amount. *See* section 28.8.
- B. “High-profit, no-risk” investments. *All* high-profit investments are inherently risky. The greater the profit, the greater the risk.
- C. High-pressure sale tactics and demands for you to “act now.” For example, the caller tells you an overnight delivery courier will quickly come to your door to collect the money.
- D. A request for your credit card number or social security number for “identification” purposes or to “verify” that you have won a prize. Indeed, it is our recommendation never to give out your credit card number over the phone unless it is you who has initiated the contact.
- E. Refusal to provide written materials or even the most basic details about the organization, such as its exact location or names of its officers.
- F. Organizations that are unfamiliar to you or that have only a post office box for an address. Some organizations use a post office box number so you will not know their exact location.
- G. Calls to you before 8:00AM or after 9:00PM. These calls violate the FTC’s Telemarketing Sales Rule (16 CFR Part 310).
- H. A call from Canada informing you that you’ve won a lottery but, for whatever reason, you must first pay some money in order to get your winnings. These calls are *always* scams. Complain to Canadian law enforcement by calling PHONE BUSTERS at 1-888-495-8501 (www.phonebusters.com).
- I. Sweepstakes promotions in which you are guaranteed to win a large prize. In fact, the odds of your winning anything of value are actually well over 1,000,000 to one. The Maine Attorney General has entered into Court ordered settlements with both Time, Inc. (2000) and Publishers Clearing House (2001) which prohibits them from using false representations to trick consumers into thinking they had won a sweepstakes (and thereby encouraging them to subscribe to magazines).

§ 28. 4. How To Avoid Becoming A Victim

To avoid being swindled, follow these precautions:

- A. Never give out your credit card number, checking account number or social security number by phone, mail or internet unless you have done business with the organization in the past and have been satisfied by its performance.⁴

⁴ Be aware that your name, Social Security number, and other personal information are now available to anyone with a credit card through a new database called P-TRAX. This information could be used to commit credit card fraud. You can have your personal information removed by making a telephone request. Call toll-free 888-965-3947. You will get a message, but do not hang up. After the message, an operator will take your request. You’ll later receive confirmation that your name has been removed from this database.

- B. Insist on getting written information about the organization. At the same time, do not assume an organization is legitimate solely on the basis of impressive-looking brochures or enthusiastic testimonials. *Always read the small print!* If you read closely you will discover that only one person in thousands receives the big prize and that all others get items worth only a few dollars (and much less than you paid).
- C. Find out if any complaints have been registered against the company with the Better Business Bureau or the Attorney General’s Consumer Mediation Service. But scam artists frequently change names and locations. Just because there are no complaints on file does not mean a business is trustworthy.
- D. In the case of charitable organizations, you have the right to know if the caller is a volunteer or a professional telemarketer/fundraiser.⁵ Do not commit yourself over the telephone. Insist on written information about how much will be spent on administrative and fund-raising costs. If they refuse to send you such information or claim they cannot afford to mail you such information, *do not* contribute.
- E. Take time to make a decision before investing. Consult someone whose financial advice you trust – a banker, lawyer, accountant or friend. Have them review any contract or prospectus before you commit yourself. For example, *never* purchase land without having an attorney review the contract and search the title first.
- F. If a caller is uncooperative in answering your questions, simply hang up the phone. Remember, you have a right to know specific facts. They have no right to your money.
- G. If you invest anyway (and we hope you do not!), keep excellent records. They might help you recover your money.
- H. If you want to greatly reduce the number of telemarketing calls you receive, sign up for the federal Do Not Call list. *See* § 28.13 in this Guide.
- I. If you want a specific company to not make telemarketing calls to you, including a charitable fund-raiser, tell the company to put your name on its “no calls” list. *See* § 28.13 in this Guide. If that company then calls you can recover your damages, up to \$500 for each violation.⁶
- J. Be wary of Automated Telephone Solicitations. These recorded messages can violate Maine law if the seller is not registered with the Secretary of State.⁷ Also, telemarketers cannot call your cell phone (10 M.R.S.A. § 1499).
- K. **Above all, remember this advice: “If it sounds too good to be true, it is not true!”**

If you have a question about whether a particular offer is legitimate, call the Maine CHECK IT OUT! Program for some quick advice at 1-877-353-3771 (toll free).⁸

§ 28. 5. Examples Of Telemarketing Fraud

Here are some common examples of telemarketing trickery (which also show up in the mail or on the internet):

- A. *Water Purifiers.* Capitalizing on growing environmental awareness, some businesses are

⁵ 9 M.R.S.A. § 5012. *See* Chapter 25, Consumer Rights and Charitable Solicitations.

⁶ 10 M.R.S.A. § 1499; *see also* 32 M.R.S.A. § 4690-A (Maine’s “Do Not Call” statute).

⁷ 10 M.R.S.A. §§1498-1499.

⁸ The Check It Out! Program is a service provided jointly by the Maine Bureau of Elder and Adult Services, the Maine Attorney General, Maine AARP and local police departments. *See also* www.maine.gov/ag/?r=protection.

selling ineffective water purification filtration systems. Callers might use scare tactics to convince you that your tap water is filled with impurities or cancer-causing substances. You may end up paying \$300 to \$500 for a device that is worth less than \$50. Be certain to ask whether the purification system deals with lead or radon, two very serious health risks.

- B. *Charities.* Some unscrupulous telemarketers will say they are calling on behalf of a charity. They may ask you to buy tickets for a benefit show, make a donation toward sending handicapped children to a circus, or purchase light bulbs or other household items at inflated prices, to cite a few recent examples. Also be suspicious of persons who claim to be calling on behalf of local law enforcement agencies. Insist on written proof that the local police are really involved.
- C. *Travel or Vacation Offers.* So-called “free” or “low-cost” vacations often come with extra charges, hidden restrictions, and hard-to-meet conditions. You might be required to join a travel club. A vacation for two may only include airfare for one. In order to receive your “free” airline ticket you might be required to purchase expensive hotel rooms.
- D. *Vitamins.* Some health conscious consumers fall prey to telemarketers selling vitamins. As with many other scams, the sales pitch may include a prize offer to get you to pay as much as \$600 for a 6-month supply of vitamins that are worth as little as \$40.
- E. *Investments.* “Get rich quick” schemes involving rare coins, gemstones, real estate, securities, oil and gas leases, and precious metals are commonly pushed on unsuspecting consumers. Almost all are worthless. Frequent targets are those who have been victimized before, since they are often eager to recoup losses from previous bad deals. Always check with the Maine Securities Division (207-624-8551) before investing in such schemes.
- F. *Recovery of Lost Money.* The latest fraud afoot is to call people who have lost money to a telemarketing or mail fraud and offer to recover the lost money—for a price. These people are often related to the very scam artist who originally took your money. That is how they knew whom to call. You will get little or nothing for your money.⁹
- G. *Cross Border Phone Calls.* You get a message urging you to call a number in 809 or another unfamiliar area code. The call may claim to concern an overdue account or a sick relative. In fact, the call is a fraud. You’re being asked to call a pay-per-call service in the Caribbean, similar to a 900 number, with charges that could top \$25.
- H. *Business Promotions.* A common telephone scam is the business promotion. The callers target the elderly and attempt to convince them that they are *guaranteed* to win one of several very valuable prizes worth thousands of dollars. All the consumer has to do is purchase a “gift pack” for several hundred dollars. Of course the “gift pack” is really worth \$25 or so and if the consumer actually receives a prize, it is worth much less than what the consumer paid.
- I. *Audiotect Services.* Some sellers of telephone-recorded messages may use unfair or deceptive tactics. Maine consumers have specified remedies to defeat such tactics. *See* 35A M.R.S.A. §§ 801-808, Collection For Audiotect Service Charges.
- J. *Automated Telephone Solicitations.* Automated telephone solicitations are regulated in Maine. *See* 10 M.R.S.A. §§ 1498-1499. For example, automated telephone calls can only

⁹ In 1996 the Attorney General charged RMS, Inc. with unfair and deceptive trade practices in a “re-loading” scheme whereby it attempted to solicit more money from consumers who had previously been the victim of telemarketing fraud, under the guise of helping the consumers get back some of the money they had previously lost. Under both a State and Federal District Court Consent Decree RMS, Inc. agreed to give back up to \$900 to each of injured consumers. *See State of Maine v. Recovery Marketing Services, Inc., et al*, No. 95-307-P-H (D. Me. July 3, 1996); *State of Maine v. Recovery Marketing Services, Inc., et al*, No. CV-94-83 (Me. Super. Ct., Kenn. Cty., June 27, 1996).

be made between 9 a.m. and 5 p.m. on weekdays, and then only for non-commercial calls.

- K. *Deceptive Prizes.* Be aware of clever sale pitches, designed to hide deceptive practices. Below are actual instructions that were given to a telemarketer who operated briefly in Maine on how to respond to a consumer's skepticism that the consumer should purchase a product in order to also receive a "top award." Such solicitations are illegal in Maine (32 M.R.S.A. § 14701 (8)). Here is the telemarketer's "script:"

Skepticism

I can appreciate your skepticism [name of consumer], all that tells me, is I'm speaking to an intelligent person. So let's speak intelligently. We're not asking you to reach into your back pocket and send us a bunch of money, and hope you get an award. There is no hope or luck involved in this promotion. That's the beauty of this promotion, as it has been predetermined that you, [name of consumer], are guaranteed to receive one of the 5 top awards in the largest promotion in our company's history. So do yourself a favor, let the promotion fall into place for yourself, and when it's all said and done you'll be calling me back to say thanks. FAIR ENOUGH?

Why Do I Have To Buy?

[name of consumer], the company asks you to place an order for two reasons, one, we couldn't use your picture saying that you are a customer of ours if you really aren't, and two, the most important reason, is because you're not taking any chances. You are guaranteed a major award. You can't lose. FAIR ENOUGH?

Guarantee

Obviously, I'm not allowed to disclose which of the awards you're to receive. I wouldn't jeopardize my position for anyone. But I can tell you this, what you'll be receiving, you'll DEFINITELY be happy with, anybody would. You did very well in this promotion.

What's The Catch/ How Much Is This Going To Cost Me?

Well, I will ask you for a small invoice, but that's not the important thing. What is important is that because you are guaranteed one of these major awards we may have to use your picture in major magazine advertisements with the item you receive. But I can assure you, that these advertisements will ONLY appear in respectable publications, like Vogue, Cosmopolitan or People. You don't have any objections to that do you?

No Money Back Guarantee

How would it look when one of our customers receives a \$5,000.00 cashier's check, and told everyone that we gave him/her a great award but he/she sent the product back. We can't give you a money back guarantee because you're guaranteed a major award, but let's say this, if you're not happy for any reason, give us a call and we'll do whatever it takes to make you happy. FAIR ENOUGH?

If you decide to back out of an investment and you demand a refund, be wary! These companies consider refund demands to be an opportunity for an even more outrageous sales pitch. Remember, they will say *anything* to get your money.

§ 28. 6. Credit Card Purchases

A. Responsibilities of Issuers of Credit Cards

What happens when you pay for your goods and services with your credit card and you then have a dispute with the merchant because you think the merchant has violated the contract by failing to deliver the goods you ordered? Any claims or defenses against the merchant, other than tort claims, can also be raised against the issuer of your credit card.¹⁰ However, before you can refuse to pay the issuer of your credit card the following requirements must be met:

- (1) The amount of initial transaction with the merchant must exceed \$50.
- (2) You must have made a good faith effort to resolve your dispute with the merchant. This can be accomplished by writing a letter to the merchant and keeping a copy of your letter as proof that you attempted to resolve your dispute.
- (3) The place where the initial transaction occurred has to have been in Maine (or within 100 miles of your Maine address). Consumers should take the position that the telephone transaction occurred in the consumer's home state, since that is where the telemarketer initiated the sale; and
- (4) Where the amount at stake is less than \$50, there are at least two approaches available to the consumer. One is notifying the card issuer under state law (*see below* § 28.6(D)) or the Fair Credit Billing Act (FCBA) that there has been a billing error.¹¹ The Federal Reserve Board has stated that the failure to provide purchased goods or services is a billing error.¹² The credit card issuer must then commence an investigation. Another approach is to commence a Maine Unfair Trade Practice action (*see* Chapter 3 in this guide) against the card issuer, claiming it is a UTPA violation for a card issuer to continue to process a telemarketer's charge if it should have known of the telemarketer's fraud.¹³

In general, when a merchant (either in-state or out-of-state) contacts a consumer in the home, either in person, by telephone or by mail, then that the transaction is taking place in the state of Maine and therefore any claims or defenses the consumer might have against the merchant can also be raised against the credit card issuer.¹⁴ Nevertheless, do not wait more than two billing periods to write to your credit card issuer and dispute the charges.

B. Common Consumer Defenses

Here are some of the most common claims and defenses you can raise against both the merchant and the issuer of your credit card:

- (1) The merchant's sales presentation either misrepresented a material fact, created an impression that was false and that the seller did not believe to be true, or made a false promise that the seller did not intend to perform or knows will not be performed.¹⁵

¹⁰ 9-A M.R.S.A. § 8-303(6). These limitations do not apply if the merchant itself issued or controls the credit cards you made the purchase with.

¹¹ *See* 15 U.S.C. § 1661; *see also* National Consumer Law Center, *Truth in Lending*, § 4.7.

¹² Official Staff Commentary, § 226.13(a)(3-1).

¹³ For example, the FTC in *Citicorp Credit Services, Inc.* (5 Trade Reg. Rep. (CCH) ¶23, 280) claimed that Citicorp should have been aware of the fraud because of a large number of consumer complaints and a 25% charge back rate (charges removed from the consumer's account and charged back to the business).

¹⁴ 14 M.R.S.A. § 704-A.

¹⁵ *See* 9-A M.R.S.A. § 5-117; the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207.

- (2) The merchant initiated the sale by contacting the consumer at home and violated either the Maine Consumer Solicitations Act¹⁶ or the Maine Transient Sales Act.¹⁷ For example, the Consumer Solicitations Sales Act requires any telemarketer to provide the consumer with a written contract that provides a three-day cancellation period, before the sale can become binding.¹⁸ Violation of either of these statutes is both an unfair trade practice and a Class D crime. *See* Chapter 13 of this Guide.
- (3) The merchant was responsible for significantly violating the contract. For example, the merchant never provided the goods or services that were described to the consumer either in the mail solicitation or the phone solicitation.
- (4) The merchant violated the FTC Mail Order Merchandise Rule (which includes telephone sales).¹⁹
- (5) The merchant violated the Maine Negative Option law, which requires telemarketers who sell goods or services with a “negative option” trial period to send to the consumer at least 15 days prior to any charge, a clearly written description of the good or service being purchased, the amount to be charged and the calendar date the consumer will be charged for the good or service if the consumer does not cancel the sale.²⁰ Violation of this law is an unfair trade practice (5 M.R.S.A. § 207).

C. Steps to Take Against the Merchant

Here are the steps you should take if you decide you have a good claim or defense against a merchant and you made the purchase by credit card:

- (1) Contact the merchant in writing and attempt to resolve the problem. There is no formal specific procedure required, only that you make an honest attempt to resolve your dispute. Remember to keep a copy of your letter.
- (2) If the merchant will not cooperate, notify the credit card company in writing that you are withholding payment for the disputed charge.
- (3) In your notification, inform the credit card company of your name, account number, the item, the reference number, the amount you are refusing to pay, why you are refusing pay, and the ways you attempted to resolve the problem. Pay the rest of the bill as usual. (Be sure to notify the credit card company within two billing periods.)
- (4) Keep in touch with the credit card company and pay the disputed amount if you still owe it once the problem has been resolved.

¹⁶ 32 M.R.S.A. §§ 4661-4671. The Maine Consumer Solicitation Sales Act applies when a salesperson contacts the consumer in the consumer’s home “by means of and including, but not limited to, a personal visit or telephone call upon the consumer...without the consumer soliciting the initial contact...” 32 M.R.S.A. § 4662. *See also* Home Solicitation Sales Act, 9-A M.R.S.A. §§3-501-3-507. This act imposes parallel requirements to credit sales that occur when the seller initiates the sale by personally contacting the consumer at home.

¹⁷ 32 M.R.S.A. §§ 14701-14716. The Transient Sales Act applies to sellers without a permanent place of business in Maine when the seller contacts the consumer by telephone or in person. It can also apply when the seller contacts the consumer by mail and offers “merchandise or money prizes as free of charge, such as contest prizes or gifts for answering a survey, but who requires the recipient to pay something of value in order to participate in this offer, including but not limited to, entrance fees, processing fees or handling charges.” 32 M.R.S.A. § 14701(8).

¹⁸ 32 M.R.S.A. § 4662.

¹⁹ *See* Chapter 12 of this Guide, § 12.3.

²⁰ 10 M.R.S.A. § 1210. In October 2001 Maine entered into a multi-state settlement against Triad Discount Buying Service, Inc., which used telemarketing and credit card fraud to deceive over 1,100 Maine consumers into purchasing memberships in a “buying club.” As a result of this multi-state action Triad was required to pay over \$8,000,000 in restitution to approximately 276,000 consumers nationwide.

D. Credit Card Billing Errors

Consumers can also challenge “billing errors” made by the issuer of the credit card.²¹ Included in billing errors are:

- (1) An inaccurate bill or an incorrect billing for a product or service the consumer never ordered; and
- (2) The billing statement that indicates that goods or services were delivered to the consumer when in fact they *were not or not delivered in accordance with the agreement* the consumer made with the seller.

If there is an error on your credit card bill, you should write to the credit card company on a separate piece of paper rather than on your bill. The letter should be sent to the listed credit card “billing error” address, stating that an error has been made. You should include:

- (1) Your name and address;
- (2) The account number; and
- (3) The nature and the amount of the error.

This notice is effective *only* if the company receives it within *60 days* of the date the bill was first sent to you. Note: your billing rights, and the billing “error” address, should be printed on the front or back of each credit card statement.²²

If your billing problem is not resolved within 30 days, the company must acknowledge your complaint and begin an investigation. Within 60 days after that the company must either correct the item or explain to you in writing why it feels the charge is correct.

You do not have to pay the amount of the bill you dispute while it is being investigated. *Please note: the portion of the bill not in dispute must be paid as usual.* However, if the investigation proves that you were wrong and the company is right, you will be expected to pay the charges as well as any additional finance charges incurred during the delay.

If you need help with your credit card complaint, contact the Maine Bureau of Financial Institutions (Consumer Outreach Program) at 207-624-8570 or 1-800-965-5235.

§ 28. 7. C.O.D. Purchases

What should you do if you have been the victim of a scam and you purchased the goods C.O.D. (collect on delivery)? If you pay by check and then discover, after opening the package that you have been tricked by the seller, you can stop payment on the check. The federal law allows recipients of C.O.D. packages to pay the charges by check made payable to the sender. Consumers can stop payment on the check if they think the goods have been *intentionally* misrepresented.

§ 28. 8. Pay-Per-Call

Pay-per-call services, such as 809 or 900 telephone numbers, are often used as part of a scam. The Federal Communications Commission and the Federal Trade Commission enacted rules prohibiting 800 numbers being used in a manner that results in a charge being assessed to the caller. Other pay-per-call numbers can still be a problem. For example, a consumer will receive in the mail an attractive announcement proclaiming that they have either won money or become eligible for a low-cost vacation. The announcement will also state that if the consumer calls a 900 number they

²¹ 9-A M.R.S.A. § 8-401; *see also* § 28.6(A)(4) in this Guide.

²² 9-A M.R.S.A. § 8-41 to 8-404.

can receive the details of their winnings. Invariably, such notices are highly deceptive. Maine has several laws that can protect consumers in such situations. These laws are:

- A. *The Maine Unfair Trade Practices Act.*²³ The Maine Unfair Trade Practices Act prohibits such trickery and allows the consumer to sue for damages or for their money back.²⁴
- B. *The Maine Transient Sellers Act.*²⁵ The Maine Transient Sellers Act requires all out-of-state sellers who use 900 numbers in the State of Maine to register with the Department of Professional & Financial Regulation as a transient seller. Such transient sellers must be licensed and bonded. A transient seller is described as “any person who engages in the business of selling merchandise to consumers by means of personal contact or telephone contact, whether or not the seller is present on the state at the time of the contract or time of sale...and who does not have any permanent place of business within the state.”²⁶
- C. *The Consumer Solicitations Sales Act* (door-to-door sellers), and the *Home Solicitation Sales Act* (credit sales).²⁷ These acts each require the seller to use a written contract with a 3 day right-to-cancel clause and prohibit sellers from:
 - (1) Misrepresenting any material fact relating to the terms or conditions of the sale;
 - (2) Creating a false impression that the seller does not believe to be true; and
 - (3) Promising performance that the seller does not intend to perform or knows will not be performed.

Further, the Federal Trade Commission has enacted a rule, pursuant to the Federal Telephone Disclosure and Dispute Resolution Act of 1992²⁸ requires a message for any 809 or 900 caller that will alert the caller to the cost of the call and give the caller an opportunity to hang up. If you have used an 809 or 900 number and feel that you have been unfairly tricked by the seller, you should complain to your telephone utility. Pursuant to Maine PUC Rule Chapter 202,²⁹ which regulates pay-per-call services, once the telephone utility receives your complaint, the utility must perform the following resolution procedures:

- A. Upon receipt of the customer’s dispute, the telephone utility must either delete the 900 service charge from the customer’s bill for basic telephone service or investigate and attempt in good faith to resolve the dispute.
- B. Any investigation, at a minimum, should include a demonstration that the 900 number seller has complied with Maine law and any rules issued by the Federal Communications Commission or any rules adopted by the Maine Attorney General pursuant to the Maine Unfair Trade Practices Act. A consumer’s telephone cannot be disconnected because of nonpayment of charges for any pay-per-call service.³⁰
- C. Another approach is to call the National Fraud Information Center at 1-800-876-7060,

²³ 5 M.R.S.A. §§ 205-A-214. Maine’s “long-arm” statute (14 M.R.S.A. § 704-A) allows enforcement against out-of-state sellers. See *Electronic Media International v. Pioneer Communications of America, Inc.*, 586 A.2d 1256 (Me. 1991).

²⁴ 5 M.R.S.A. § 213.

²⁵ 32 M.R.S.A. §§ 14701-14716.

²⁶ 32 M.R.S.A. § 14701(8). Further, it is a violation of the Transient Sellers Act if the seller sells exclusively by mail contact and offers “merchandise or money prizes as free of charge, such as contest prizes or gifts for answering a survey, but then requires the recipient to pay something of value in order to participate in this offer, including but not limited to, entrance fees, processing fees or handling charges.” We consider the cost of an 800 or 900 number to be the equivalent of a processing fee.

²⁷ See 32 M.R.S.A. §§ 4661-4671; 9-A M.R.S.A. §§ 3-50-3-507.

²⁸ 470 U.S.C. § 228; see related rules at 16 C.F.R. Part 308.

²⁹ This PUC Rule applies to any telephone informational or other service number for which, in addition to any basic service charge, a fee is charged on a per-call or per-minute basis or some combination thereof.

³⁰ 47 U.S.C. §228 (C)(4); 47C.F.R. 64.1507; 35A M.R.S.A. § 802 (Collection For Audiotest Service Charges).

which was established by a coalition of groups battling telephone fraud. The line is open from 9:30 a.m. to 5:30 p.m.

§ 28. 9. Automatic Checking Account Debit Scams

Consumers frequently report that they have had money automatically withdrawn from their checking account without their permission. These electronic withdrawals are part of an automatic debit scam. *Never give out your checking account number.* A telemarketer may ask you to read out all the numbers at the bottom of your check, saying this information is necessary to ensure you will qualify for the offer. Once a telemarketer has your checking account number, he can present a “demand draft” to your bank. This draft is processed like a check, but does not require your signature. You may not know your bank has paid the draft until you receive your bank statement. Consumers can challenge such electronic withdrawals. If your bank cannot produce verifiable authorization, the bank must refund the money to the consumer. Your bank can then seek reimbursement from the telemarketer’s bank that accepted any unauthorized deposit.

§ 28. 10. Protections Against Fraudulent Telemarketers

Both Maine and Federal law protect consumers from unfair telemarketer sales pitches. Maine’s Consumer Solicitation Sales Act is particularly important because it requires that telemarketers who initiate the sale by calling you at home must provide you with a written contract that gives you three days to back out of the sale. This section will first discuss Maine law and then the Federal telemarketing law. *See* § 28.8, Pay-Per-Call, for a description of the Maine laws that protect consumers from fraudulent telephone charges.

The Federal Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 required³¹ that the FTC issue Rules prohibiting various deceptive and abusive telemarketing practices.³² They regulate campaigns to sell goods or services that involve more than one interstate telephone call. The Rules do not distinguish between seller-initiated calls and calls initiated by the consumer in response to a solicitation. However, the Rules do not usually cover sales in which the consumer calls the seller after seeing an advertisement or catalogue.³³ Here is a summary of some of the more important FTC Rule’s Provisions:

- A. It is illegal for telemarketers to call you if you have asked not to be called or have placed your name on the Maine or Federal Do Not Call list.
- B. Calling times are restricted to hours between 8:00 a.m. and 9:00 p.m.
- C. Telemarketers must tell you it is a sales call, the name of the seller, and what they are

³¹ 15 U.S.C. § 6102.

³² 16 C.F.R. Part 310 (revised as of January 1, 2003).

³³ Here is a listing of sellers exempted from the FTC Rule: a non-profit organization; an investment broker/firm/adviser regulated by other federal laws; a common carrier, bank and other financial institutions, and a business of insurance; an entity covered by FTC Pay-Per-Call Rule or FTC Franchise Rule. Also exempted is a call made by consumer not based on any solicitation; transaction completed face-to-face; a call made by consumer in response to media ad except if for investment opportunity, credit repair, recovery service, or promise of obtaining credit or guarantee or implication of a high likelihood of success and an advance fee is required. A call made by consumer in response to direct mail solicitation is covered except if certain disclosures are made but no exemption if solicitation relates to prize offer, investment opportunity, credit repair, recovery service or promise of obtaining credit or guarantee or implication of high likelihood of success and an advance fee is required. A call between telemarketer and a business is exempt except one involving retail sale of non-durable cleaning or office supplies.

selling before they make their sales pitch. If it is a prize promotion, they must tell you that no purchase or payment is necessary to win.

- D. It is illegal for telemarketers to misrepresent any information; any facts about their goods or services; earnings potential; profitability, risk or liquidity of an investment; or the nature of a prize-promotion scheme.
- E. Before you pay, telemarketers must tell you the total cost of the goods and any restrictions on getting or using them; or that a sale is final or nonrefundable. In a prize promotion, they must tell you the odds of winning, that a purchase or payment is not necessary to win and will not increase your chances of winning, and any restrictions must be made clearly and conspicuously and before the consumer pays anything.³⁴ Misrepresentations regarding these or other aspects of a prize promotion are also forbidden.
- F. Telemarketers must receive your “express, verifiable authorization” for all transactions, except when you are protected by credit card or debit card laws. For example, it is illegal for telemarketers to withdraw money from your checking account without your express, informed authorization.
- G. Telemarketers cannot lie to get you to pay, no matter what method of payment you use.
- H. You do not have to pay for credit repair, money recovery services or advance-fee loans/credit services until these services have actually been delivered.
- I. It is illegal to help deceptive telemarketers if you know – or consciously avoid knowing – that they are breaking the law.
- J. If the telemarketer has your account information before the call and offers you goods on a free trial basis (a “free-to-pay conversion”) the telemarketer must (1) get your permission to use a particular account number, (2) ask you to confirm the number by repeating the last 4 digits, and (3) for your protection, record the entire phone conversation.³⁵
- K. After January 29, 2004, telemarketers must transmit their phone number and if possible, their name to your caller ID service.

The Maine Attorney General can enforce both the federal FTC Telemarketing Rule and Maine’s telemarketing laws. Penalties of up to \$10,000 can be levied for each violation.

§ 28. 11. Slamming and Cramming

“Slamming” is a term used to describe any practice that changes a consumer’s long distance carrier without the customer’s knowledge or consent. Slamming is illegal and the Federal Communications Commission (FCC) will vigorously respond to any consumer complaints. The FCC has issued rules to protect consumers from slamming. Consumers are absolved of all charges incurred through the slammer during the first 30 days of service after the slam if the consumer immediately contests the charges.³⁶ When the consumer does not learn of the slam within the 30-day period because of a lack of notice or an irregular billing cycle, the consumer is directed to file a

³⁴ 16 C.F.R. § 310.3 (a) (1).

³⁵ Maine has enacted additional protections for consumers who agree to a “free” trial period. The seller must mail a complete description of the negative option sale and the deadlines after which the consumer will be charged for the good or service. See 10 M.R.S.A. § 1210.

³⁶ 47 CFR § 64.1100 (d)

petition with the FCC for a longer absolution period. Maine has its own statutory protections against slamming, which are enforced by the Maine Public Utilities Commission³⁷. Here is how to file a slamming complaint:

- A. There is no special form to fill out to file a complaint with the FCC. Simply send a letter in your own words, to the address below. Your complaint letter should include:
- (1) Your name and address, the telephone number that was “slammed,” and a telephone number where you can be reached during the business day.
 - (2) The names of your local and preferred long distance telephone companies and the long distance company to which your service was changed without your knowledge or permission.
 - (3) The names and telephone numbers of the telephone company employees with whom you spoke in an effort to resolve your complaint, and the dates on which you spoke with them.
 - (4) Any other information that you feel would help the FCC to handle your complaint. Copies of any documents you received, such as a bill for changing to the unauthorized long distance company, a bill from the unauthorized company or its billing agent, a contest entry blank, or a check.
- B. Send your complaints to:

Maine Public Utilities Commission
18 State House Station
Consumer Assistance Division
Augusta, Maine 04333-0018
1-800-452-4699

and

Federal Communications Commission
Common Carriers Bureau
Consumer Complaints
Mail Stop 1600A2
Washington, D.C. 20554

The FCC Consumer Complaint Service phone number is 202-623-7553. The FCC National Call Center can be reached *toll free* at 888-225-5322 or 888-Call FCC.

Also be alert to “cramming:” the addition of charges to your telephone bill you never agreed to (e.g., charges for voice mail, paging, club memberships, etc.). In general, consumers cannot be held liable for services they never agreed to purchase. If you’ve been crammed, call the company that billed you and complain. Also, you can tell your local phone company that provides the billing service that you are disputing the charges and that you will deduct them from your bill payment. Your phone service cannot be shut off for refusing to pay unauthorized charges. Maine has adopted statutory prohibitions against “cramming,” which are enforced by the Maine Public Utilities Commission.³⁸ Violations would also be unfair trade practices (5 M.R.S.A. § 207).

§ 28. 12. Identity Theft

Identity theft is when a person illegally steals personal information about you that can give them access to your money. If a crook can obtain your credit card number, your social security number,

³⁷ 35A M.R.S.A. § 7106

³⁸ 35A M.R.S.A. § 7107

your bank account number or other personal financial information, the thief can then use this information to make unauthorized charges or to gain direct access to your money. In 2001 identity theft was, by far, the most frequent consumer fraud complaint received by the Federal Trade Commission. Of all the complaints received (204,000), 42% dealt with identity theft. The next most common complaint involved Internet auctions (10%).

A. What Do Identity Thieves Do With Your Information?

Here are some of the identity thief scams:

- (1) They open a new credit card account, using your name, date of birth, and social security number. When they use the credit card and do not pay the bills, the delinquent account is reported to *your* credit report.
- (2) They call your credit card issuer and, pretending to be you, change the mailing address on your credit card account. Then, your imposter runs up charges on your account. Because your bills are being sent to a new address, you may not immediately realize there is a problem.
- (3) They establish a cellular phone service in your name and then make numerous, expensive calls.
- (4) They open a bank account in your name and write bad checks on that account. If they find out your checking account number, they can gain access to your bank account and drain it of its funds.

B. How Do They Steal Your Identity?

How is your personal financial information stolen? Unfortunately, it is often stolen simply by a telephone call that tricks you into disclosing your social security number or your checking account number or your credit card number. For example, one case involved telephone calls to elderly persons who were falsely told that they had won a California sweepstakes but that they had to first provide their bank account numbers to ensure payment of California taxes. Of course, the thieves used the bank account number to steal money. Here are some more sophisticated ways your identity can be stolen:

- (1) **Check Fraud:** Someone steals checks from your home, office or mailbox and forges your signature. Crooks do not need blank checks to pull off a check fraud. Many know how to easily remove the ink on checks, often by “washing” them with a cleaning solvent. They will also alter what has already been written, such as changing a check payable to the IRS to one payable to JR Smith. A counterfeiter can also make new checks in your name using a home computer and a printer. Here are some warning signs: You notice some checks are missing from your checkbook or your reserve supply of checks. Mail containing checks or bank account information is “lost” or appears to have been tampered with. You spot unauthorized transactions on your bank statement.
- (2) **Credit Card Fraud:** There are hundreds of ways thieves can use your credit card to take your money. Here are just a few. A thief may steal your credit card. Someone may order a new credit card in your name by stealing a pre-approved application from your mail and having the card sent to a different address. An unscrupulous sales clerk can make a duplicate copy of your credit card receipt or use a special device to capture data from the magnetic strip on your card. One way or another, the thief using a phony ID can make or order

a credit card, in your name, and use it to obtain merchandise or cash advances. Here are some warning signs:

- (a) unauthorized charges appear on your credit card statement or you get a statement for a credit card you did not request;
 - (b) your mail appears to have been tampered with;
 - (c) mail containing a new credit card or a credit card statement does not arrive as expected.
- (3) **ATM theft:** Sophisticated thieves will watch the victim use the ATM card (perhaps even with high-powered binoculars) and learn the persons card number and personal identification number (PIN). Later, they will steal the card or make their own and go to the ATM for cash. Here are some warning signs: One or more persons loitering around the ATM, often in a car, behind bushes or otherwise nearby. Or you spot unauthorized ATM withdrawals on your bank statement.

C. *How Can You Protect Yourself From Identity Theft?*

The US Postal Inspection Service has a variety of suggestions as to how you can protect yourself from identity theft:

- (1) Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, or bank PIN code, *unless you initiated the phone call*. Protect this information and release it only when absolutely necessary.
- (2) Shred pre-approved credit applications, credit card receipts, bills, and other financial information you do not want before discarding them in the trash or recycling bin.
- (3) Empty your wallet of extra credit cards and IDs, or better yet, cancel the ones you do not use and maintain a list of the ones you do.
- (4) Order your credit report from the 3 credit bureaus once a year to check for fraudulent activity or other discrepancies (*see below* paragraph 18 for the credit bureau addresses and phone numbers).
- (5) Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gasoline pumps. Keep track of all your paperwork. When you no longer need it, destroy it.
- (6) Memorize your social security number and all your passwords. Do not record them on any cards or on anything in your wallet or purse.
- (7) Sign all new credit cards upon receipt.
- (8) Save all credit card receipts and match them against your monthly bills.
- (9) Be conscious of normal receipt of routine financial statements. Contact the sender if they are not received in the mail (it may mean that someone has taken them out of your mailbox).
- (10) Notify your credit card companies and financial institutions in advance of any change of address or phone number.
- (11) Never loan your credit card to anyone else.

- (12) If you apply for a new credit card and it has not arrived in a timely manner, call the bank or credit card company involved.
- (13) Report all lost or stolen credit cards immediately.
- (14) Closely monitor expiration dates on your credit cards. Contact the credit card issuer if replacement cards are not received prior to the expiration dates.
- (15) Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.
- (16) Keep thieves from turning your trash into their cash. Thieves known as “dumpster divers” pick through the garbage looking for credit card applications and receipts, cancelled checks, bank statements, expired charge cards and other documents or information they can use to counterfeit or order new checks or credit cards.
- (17) Pay close attention to your bank account statements and credit card bills. Contact your financial institution immediately if there is a discrepancy in your records or if you notice something suspicious, such as a missing payment or an unauthorized withdrawal. While federal and state laws may limit your losses if you are victimized by a bank fraud or theft, sometimes your protections are stronger if you report the problem quickly and in writing.
- (18) Review your credit report approximately once a year. Your credit report (prepared by a credit bureau) will include identifying information (such as your name, address, social security number, and date of birth) as well as details about credit cards and loans in your name and how bills are being paid. You should make sure that the report is accurate; you should also monitor it for unauthorized bank accounts, credit cards and purchases. Also look for anything suspicious in the section of your credit report that lists who has received a copy of your credit history. There are at least 2 reasons why:
 - (a) First, identity thieves sometimes will fraudulently obtain credit reports – invaluable details that could be used in a financial scam – by posing as a landlord, employer or someone else who has a legal right to the information.
 - (b) Second, crooks sometimes apply for loans or apartments in someone else’s name as a way to test that person’s vulnerability. An inquiry to a credit bureau about a loan or a lease you did not apply for could be a sign that a thief is “casing” your credit history to see if you have the right background to be a potential target.

To order your credit report, call the 3 major credit bureaus at these toll-free numbers:

- (a) Equifax (PO Box 740241, Atlanta, GA 30374-0241): 1-800-685-1111;
- (b) Experian Information Solutions (formally TRW) (PO Box 949, Allen, TX 75013-0949): 1-888-397-3742; and
- (c) TransUnion (PO Box 1000, Chester, PA 19022): 1-800-916-8800.

In Maine, in any 12-month period the first copy of your report is free and the second copy cannot cost more than \$5. To be safe, consider getting a copy

from each of the 3 companies. *If after reviewing your report you spot signs of possible fraud, contact these credit bureaus.*

D. If Your Identity Has Been Stolen, What Should You Do?

If you conclude that a thief has stolen important financial information from you, there are a variety of steps you should immediately take. Here they are:

- (1) Immediately call the fraud unit of any one of the 3 credit reporting companies (*see above* paragraph C(18)). Ask that your file be flagged with a fraud alert. Add a victim statement to your report (“My ID had been used to apply for a credit fraudulently. Contact me at [your phone number] to verify all applications.) The credit reporting agency must then pass on your fraud alert to all other nationwide consumer reporting companies. Ask how long the fraud alert is posted on your file and how you can extend it if necessary. At the same time, ask the credit bureaus for copies of your credit reports. Credit bureaus must give you a free copy of your report if your report is inaccurate because of fraud. Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. Also check the section of your report that lists “inquiries.” Where “inquiries” appear from the companies that opened the fraudulent account, request that these “inquiries” be removed from your report. In a few months, order new copies of your reports to verify your corrections and changes and to make sure no new fraudulent activity has occurred.
- (2) Second, contact the creditors for any accounts that have been tampered with or opened fraudulently. Creditors can include credit card companies, phone companies and other utilities, and banks and other lenders. Ask to speak with somebody in the security or fraud department of each creditor and follow up with a letter. It is particularly important to immediately notify the *credit card issuing bank* in writing because that is the procedure the Fair Credit Billing Act spells out for resolving errors on credit card billing statements. Immediately close accounts that have been tampered with and open new ones with new Personal Identification Numbers (PINs) and passwords. Here again, avoid using easily available information like your mothers maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- (3) File a report with your local police or the police in your community where the identity theft took place. Get a copy of the report in case the bank, credit card company or others need proof of the crime. Also file a report with the FTC at www.consumer.gov/idtheft.
- (4) If an identity thief has stolen your mail in order to get new credit cards or similar items, report it to your local postal inspector. Contact your local post office for the phone number for the nearest postal inspection office. For Maine, the address is: U.S. Postal Inspector, Fraud Complaints, Gateway 2 Center 9th Floor, So. Newark, NJ 07175-003 (201-693-4520).
- (5) If the identity thief has changed the billing address on an existing credit card account, close the account immediately.
- (6) If you have reason to believe that an identity thief has tampered with your bank accounts, checks or ATM card, close the accounts immediately. In

addition, if your checks have been stolen or misused, stop payment. Also, contact the major check verification companies to request that they notify retailers using their databases not to accept these checks, or ask your bank to notify the check verification service with which it does business. Three of the check verification companies that accept reports of check fraud directly from consumers are:

- (a) Telecheck: 1-800-710-9898;
 - (b) International Check Services: 1-800-366-5010;
 - (c) Equifax: 1-800-437-5120.
- (7) If an identity thief has established new phone service in your name, is making unauthorized calls that seem to come from – and are billed to – your cellular phone or is using your calling card and PIN, contact immediately the Consumer Complaint Office at the Maine Public Utilities Commission: 1-800-452-4699; 287-3831.
 - (8) If your social security number has been misused, call the Social Security Administration to report fraudulent use of your SSN. As a last resort, you might want to change your number, although we do not recommend it except for the most serious cases.
 - (9) You may need to change your driver’s license number if someone is using yours as an ID on bad checks or for other types of fraud. Call the Department of Motor Vehicles to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV office to request a new number.

E. Additional Information About Stopping ID Theft

Here are the Federal and State Government Agencies that have publications, web sites, staff and other resources that help answer your questions on ID theft and other financial fraud:

- (1) Federal Regulators of Depository Institutions:
www.fdic.gov/consumers/consumer/news/index.html
- (2) The Federal Trade Commission:
www.consumer.gov/idtheft
- (3) The US Department of Justice and the FBI:
www.usdoj.gov/criminal/fraud/idtheft.html
- (4) The Social Security Administration:
www.ssa.gov

§ 28. 13. “Do Not Call” List (And Do Not Mail)

The Federal Trade Commission (FTC) has created a Do Not Call Registry, which makes it easier for you to stop getting telemarketing sales calls you do not want. You can register online at DONOTCALL.GOV or by phone, toll free, by calling 1-888-382-1222, TTY 1-866-290-4236 from the number you wish to register. Registration is free. Maine also has a Do Not Call list. Any names and numbers placed on Maine’s list will also be placed on the FTC Do Not Call list. We suggest you enter your name on **both** Do Not Call Lists. Here is the FTC’s explanation of how its Do Not Call list operates:

- A. **When did the National Do Not Call Registry take effect?** The FTC and the states began enforcing the National Do Not Call Registry on October, 17, 2003. That's when consumers on the registry by August 31, 2003 will notice a reduction in the number of telemarketing calls they get.
- B. **What does registration entail?** If you register by phone, you must call from the number you want to register. If you register online, you must provide an email address for confirmation. You will have to open an email and click on the line in it within 72 hours for your online registration to be complete. The only identifying information that will be kept in the registry will be the phone number you register. You can expect fewer calls within *three months* of the date you sign up for the registry.
- C. **How does the FTC Do Not Call Registry Work?** Your number will stay in the registry for five years, until it is disconnected, or until you delete it from the registry. After five years, you may renew your registration. The law requires telemarketers to search the registry. The law requires telemarketers to search the registry every three months and synchronize their call lists with the phone numbers that are on the registry. If you receive telemarketing calls after you have registered your telephone number and it has been in the registry for three months, you can file a complaint at DONOTCALL.GOV or by calling 1-888-382-1222, TTY 1-866-290-4236. You will have to know the company's name or phone number to file a "do not call" complaint. A telemarketer who disregards the National Do Not Call Registry could be fined up to \$11,000 for each call.
- D. **Will the FTC Do Not Call Registry cover all telemarketing calls?** Yes. Placing your number on the FTC Do Not Call Registry will stop most telemarketing calls, but not all. Some types of calls are exempt. Political organizations and charities are permitted to call you. Organizations with which you have an established business relationship can call you for up to 18 months after your last purchase, payment or delivery – even if your name is on the FTC Do Not Call Registry. And companies to which you've made an inquiry or submitted an application can call you for three months. However, your request to a company not to call you trumps an existing business relationship. That is, if you ask a company not to call you, it must honor your request, regardless of an established business relationship.
- E. **What about profession charitable fun-raisers?** Although callers soliciting charitable contributions do not have to search the national registry, a for-profit telemarketer calling on behalf of a charitable organization must honor your request to be on its do not call list.
- F. **Does this law apply to in-state callers?** Yes. When Maine businesses call Maine residents they must honor the FTC Do Not Call list.
- G. **How can you complain?** If you continue to get calls after you've placed your name on the FTC Do Not Call list (remember, it takes about *3 months* before the list has an effect), file a complaint with the FTC by calling 1-888-382-1222 and give the name or phone number of the company that called, the date and time of the call, and the phone number you registered on the Do Not Call list.

You can also remove yourself from **mailing lists** by sending your name, address, telephone number, *and your signature* to:

Mail Preference Service
Direct Marketing Association (DMA)
PO Box 9014
Farmingdale, NY 11735-9014

By placing your name in the DMA Do Not Mail List you can expect within a few months to receive considerably fewer unwanted mailings. Your name remains on the list for five years. After that, you must repeat the process if you want to continue to be listed. For more information see www.the-dma.org.

Consumer Credit Reporting Agencies will also sell your name to merchants. To remove your name from the mailing lists sold by credit reporting agencies call 1-888-5OPTOUT (1-888-567-8688) or write:

TransUnion LLC's Name Removal Option
PO Box 97328
Jackson, MS 39288-76328

Include your full name, current and recent addresses, Social Security Number, date of birth, and signature.

§ 28.14. Agencies Which Can Help You

As discussed above, consumers have many protections against mail order or telemarketing fraud. As explained in § 28.6, if you have been the victim of a scam and you made your purchase by credit card, then you may very well be able to force the credit card company to not charge you. If you have lost money due to a 900 or 800 telephone number scam then, as explained in § 28.8, you can explain to your phone company or the PUC and have any suspicious charges investigated. If you do get swindled, do not be embarrassed to report it or assume it's not worth your time. By reporting the incident, you can help assure that others are not victimized. Here are some agencies you should contact:

- A. *The Attorney General's Consumer Division.* Contact the Consumer Protection Division in the state in which the mail-order seller or telemarketer is located. See Chapter 30 of this Guide, § 30.4 for a listing of each state's Attorney General's Consumer Protection Division. When you write to these sellers make sure that you indicate in your letter that you are also complaining to the Attorney General's Office in the state in which they are operating. Then send a copy of your letter to that Attorney General.
- B. *The Public Utilities Commission.* The Maine PUC has a consumer complaint division (207-287-3831). Complain to the PUC about any fraudulent schemes that use the telephone, such as a deceptive 900# scheme.
- C. *Your Telephone Company.* Always complain to your telephone company about a fraudulent scheme conducted over the phone. It will investigate and not charge you if you have been the victim of a scam.
- D. *Federal Trade Commission.* You should also contact the Telemarketing Fraud Division of the Federal Trade Commission: Room 200, 6 Pennsylvania Avenue, N.W., Washington, DC 20580. (www.ftc.gov/bcp/online)

- E. *Alliance Against Fraud in Telemarketing.* This agency is located at 815 15th Street, N.W., Ste. 516, Washington, DC 20005.
- F. *Better Business Bureau.* Contact your local BBB. For the phone number of an out-of-state BBB call the Counsel of Better Business Bureaus at 702-276-0100.
- G. *North American Securities Administration Association.* For the address and phone number of any state Securities Divisions call 202-737-0900. State Securities Divisions enforce laws concerning the sale of stocks, bonds, investment opportunities and the like. The phone number of the Maine Securities Division is 207-624-8551.
- H. *U.S. Postal Service.* The U.S. Postal Service investigates and pursues complaints about bogus mail order investments and other businesses that use, advertise or sell through the mail. This includes telephone solicitors and newspaper advertisements because money sent in response to them is usually mailed. Contact your local postmaster or postal inspector. The number can be found in your telephone book under U.S. Government, Postal Service. See § 30.5 of this Guide for a listing, by region, of the U.S. Postal Inspectors.
- I. *National Futures Association.* The National Futures Association is a self-regulatory organization for all registered individuals or brokerage firms selling commodity futures such as sugar, gold, petroleum, soybeans, and foreign currencies. To report fraud, write National Futures Association, 200 W. Madison Street, Ste. 1600, Chicago, IL 60606 or call toll free 1-800-621-3570.
- J. *National Fraud Information Center.* This Center is operated by the national Consumer League and offers telephone guidance as to whether a particular solicitation is fraudulent. Call 1-800-876-7060 between 9:00 a.m. and 5:30 p.m.
- K. *Federal Communications Commission.* The FCC has a National Call Center, which provides consumer information on telephone-related issues, including “do not call” complaints. It can be reached by calling 1-888-225-5322.

§ 28.15. E-mail Spam

The federal government has recently enacted the CAN-SPAM Act of 2003 to help protect consumers from unwanted E-mail spam. This new law:

- A. Prohibits senders from falsifying or disguising their true identity;
- B. Prohibits businesses from using misleading subject lines;
- C. Requires the inclusion of a legitimate return E-mail and physical postal address, an opt-out mechanism, and notice of the opportunity to opt-out;
- D. Requires clear notice if message is an advertisement or solicitation or has sexually oriented material.

Violations can result in civil damages for as much as \$250 per spam E-mail. Individual consumers can't sue spammers, but the new law empowers internet service providers to do so. If you have a specific complaint about unsolicited E-mail spam, you can forward the spam directly to the Federal Trade Commission at UCE@FTC.gov.

In addition to the requirements of this federal law, a spam message that is unfair or deceptive can also be a violation of the Maine Unfair Trade Practices Act (5 M.R.S.A. § 207).