



Karl A. Racine
Attorney General

Office of the Attorney General for the District of Columbia

PROTECT YOURSELF: **A CONSUMER PROTECTION** **GUIDE**



Connect with the Office of the Attorney General
441 4th Street, NW, Washington, DC 20001
CONSUMER HOTLINE - (202) 442-9828

NOTES

[illegible]

Dear D.C. Consumer:

This consumer protection guide is designed to help you avoid some of the problems consumers routinely face. Unfortunately, everyday activities – such as answering the phone, responding to an email, or making a purchase – can expose consumers to scams like identity theft, aggressive telemarketing, and charity fraud. The good news is that the Attorney General's Office of Consumer Protection can help.

This guide contains information and tools to help you protect yourself before something happens. However, should you or a loved one become a victim of a scam, our office has a dedicated team of lawyers, investigators, and mediators who are here to help. Should you need our assistance, please call (202) 442-9828. You can also file a complaint online by emailing consumer.protection@dc.gov or writing to: the Office of the Attorney General's Office of Consumer Protection, 441 4th Street, NW, Washington, DC 20001.

Sincerely,



Karl A. Racine

Attorney General for the District of Columbia



CONTENTS:

<i>Telemarketing Scams</i>	5
<i>Money Transfer Scams</i>	7
<i>Online Privacy and Identity Theft</i>	9
<i>Debt Collection</i>	12
<i>Debt Relief</i>	13
<i>Home Improvement Abuse</i>	14
<i>Buying a Home</i>	16
<i>Health Care Fraud</i>	17
<i>Health Products/Weight Loss</i>	18
<i>Hearing Aids</i>	19
<i>Living Trusts/Funeral Expenses</i>	20
<i>Charity Scams</i>	21
<i>Sweepstakes/Prize Scams</i>	22
<i>Timeshare and Travel Scams</i>	23
<i>Car Purchases</i>	24
<i>Investment Scams</i>	26
<i>Financial Exploitation</i>	27
<i>Helpful Resources</i>	29



TELEMARKETING SCAMS

Y*ou get a call almost every evening offering to lower your credit card rate or describing a “limited time” offer. While there are many trustworthy companies that use the telephone for marketing, it’s sometimes hard to tell the difference between a reputable telemarketer and a con artist who uses the phone to take your hard-earned money.*

- Don’t be afraid to hang up if you feel pressured or the telemarketer is not answering your questions.
- Do not give out your bank account number or other personal information over the phone. Your bank, credit card company, or broker will not call you to ask for your account or Social Security number. Typically, they will only ask for such identifying information when you call them.
- Avoid high-pressure offers that require you to act immediately. Legitimate merchants will give you time to consider their offers.
- Avoid returning calls to unknown area codes. Calling back an unknown area code can be expensive because merchants may be located in Canada or the Caribbean, where they also use three-digit area codes. A call lasting just a few minutes could cost you \$20 or more.



How to stop unwanted telemarketing calls and junk mail

Register on the “Do Not Call” List. You can stop many unwanted telemarketing calls by adding your phone number to the National Do Not Call Registry either by calling (888) 382-1222 or visiting www.donotcall.gov to register your phone number; include both your home and mobile phone. You can also ask callers to put your phone number on their internal do-not-call lists.

Call Blocking. Unwanted calls to landlines can be blocked through accessories that may already exist in your phone or may be available from your phone company. For cell phones, there are a number of apps that may be purchased to block calls, such as “Nomorobo.” You can also check your phone’s settings to see what blocking features you already have.

Register with the Direct Marketing Association's Mail Preference Service. To have your name removed from many national mailing lists, you can call (212) 768-7277, ext. 1888 or register online at www.dmachoice.org.

Tell the credit reporting agencies that you don’t want to receive pre-approved offers of credit. You can tell all three of the major credit reporting agencies (Equifax, Experian, and TransUnion) to remove your name from their mailing lists by calling one toll-free number, (888) 5-OPT-OUT (888-567-8688). You can have your name removed for 5 years.



MONEY TRANSFER SCAMS

M*any scammers ask consumers to send money by wire transfer through companies like Western Union and MoneyGram. If you wire money and receive nothing in return, you may not be able to recover your money, as many scammers are located in foreign countries. Here's how you can protect yourself:*

- Never use money (wire) transfers to send funds to people or companies you don't know.
- It is always better to make payments with a credit card if you are financially able to do so. You are only liable up to \$50 for fraudulent transfers and most credit card companies will provide full refunds if you have been a victim of a scam.
- Don't trust a company that sends you a check – even a bank or cashier's check – and asks you to wire funds back after you deposit the check. Even if your bank accepts the check for deposit, it could still be a counterfeit check that never clears.
- Avoid purchasing any product online if the only accepted method of payment is a money transfer.

(Continued on the next page)



- Be wary of someone who calls or emails you claiming to be a relative in need of a money transfer unless you are sure you know the caller or sender is who they are claiming.
- Don't respond to calls or emails from strangers asking you to "help" a person located in another country transfer money out of his or her homeland – the so-called "Nigerian Lottery Scam." If an offer sounds too good to be true, it probably is.
- If renting an apartment or house, never wire money to pay for an application fee, security deposit, or first month's rent without visiting the apartment and talking to the landlord.
- Do not provide the routing and account numbers at the bottom of your checks to telemarketers who call you. Those numbers may be used to withdraw money from your account.

If you've fallen victim to a money transfer scam, immediately contact the company through which you sent the money. If it is not too late, you can ask for the money transfer to be reversed. You can reach the complaint departments of MoneyGram at (800) 666-3947 and Western Union at (800) 448-1492.



ONLINE PRIVACY AND IDENTITY THEFT

If you find unexplained withdrawals from your bank account, or receive bills or charges for services you never purchased, you may be a victim of identity theft. If you believe your identity has been stolen, you should immediately:

Contact your financial institutions. Call the phone numbers on your bank account statements and on the backs of your credit and debit cards to alert them of any fraudulent charges or withdrawals.

Order Your Credit Reports for Free. Visit www.annualcreditreport.com or contact the three national credit reporting agencies at:


- ⇒ TransUnion: (800) 680-7289, transunion.com, P.O. Box 6790, Fullerton, CA 92834-6790
- ⇒ Experian: (888) 397-3742, experian.com, P.O. Box 9532, Allen, TX 75013
- ⇒ Equifax: (800) 525-6285, equifax.com, P.O. Box 740241, Atlanta, GA 30374-0241

Place a Fraud Alert. Visit www.consumer.ftc.gov/articles/0275-place-fraud-alert or contact the three national credit reporting agencies.

Create an Identity Theft Report. Visit: www.identitytheft.gov or call the Federal Trade Commission at (877) 438-4338 and the Financial Crimes and Fraud Unit of the D.C. Metropolitan Police Department (MPD) at (202) 727-4159.



Protect yourself from identity theft:

Use only “secure” sites when shopping online or providing information about yourself. These sites have an  icon in the status bar, and their address (or URL) begins with “https.”

Keep personal records in a secure place and shred them once they are no longer needed.

Before sharing personal information, ask why it is needed and how it will be safeguarded.

Do not leave mail unattended in an unlocked mailbox. Have the Post Office hold your mail if you will be away from home for several days or more.

Destroy labels on your prescription bottles before throwing them away.

Keep your computer and mobile devices up to date with antivirus protection.

Remove personal information from computers or mobile devices before selling them or throwing them away.

If you receive an email requesting personal information – even one from a company you trust – do not click on links in the email, as the email may be a fake. Instead, use your Internet browser to find the company’s website.

Immediately report lost or stolen ATM/bank/credit cards to the cards’ issuer.



The IRS does not use phone calls, emails, texts, or social media to make initial demands on taxpayers. Report suspicious messages appearing to be from the IRS to phishing@irs.gov or (202) 803-9000.

Similarly, banks or credit card companies ordinarily will not ask for personal or account information via an email.



DEBT COLLECTION

If you owe money to a creditor, a debt collector may contact you seeking payment. You have rights not to be unduly pressured and to ask for verification to assure yourself that the debt sought to be collected on is valid.

Even if attempting to collect a debt that you do owe, a debt collector may not:

- ⇒ Harass you with excessive phone calls, calls outside the hours of 8 a.m. to 9 p.m., obscene language, or threats of arrest.
- ⇒ Reveal your identity to anyone other than the credit reporting agencies.
- ⇒ Make false claims relating to their identity or the amount of debt that you owe.
- ⇒ Collect any interest or fee not authorized by the contract creating the debt.



As a consumer, you have the right to:

- ⇒ Make a written request for a validation of your debt.
- ⇒ Ask for specification about which debt your payment will go toward (if you owe multiple debts to the same creditor).
- ⇒ Make a written request stating that you do not wish to be contacted. After such a request, the collector may not contact you except to let you know that the collector or the creditor intends to take a specific action, like filing a lawsuit.



DEBT RELIEF

The airwaves are full of advertisements from companies claiming they can lower or eliminate your credit card debts, amounts owed for student loans, or tax debts.

Before hiring a company to assist you with any debts, you should consider the following:

Avoid companies that require you to pay large up-front fees. There are a number of federal and state laws that bar debt relief companies from charging a fee until all promised services have been performed.

If you want to consult with a credit counseling agency, check your local bankruptcy court to see if it has been approved by the United States Trustee (<https://www.justice.gov/ust/list-credit-counseling-agencies-approved-pursuant-11-usc-111>) or whether it is a member of the National Foundation for Credit Counseling.

You can first call your credit card company before hiring a debt relief agency. Many credit card companies will work with consumers to resolve their debt situation.

If you are having trouble paying your **student loans**, you can first call the U.S. Department of Education to see if you are eligible to consolidate your loans or get other relief. Call (800) 433-3243 or visit <https://studentaid.ed.gov/sa/repay-loans/>.



HOME IMPROVEMENT ABUSE

Remodeling or performing construction on your home may require a contractor. There are a few things you can do to ensure that you find someone reputable:

Research contractors before hiring them. Find out whether a contractor's license is valid and up to date. To verify a D.C. contractor's license, call the Department of Consumer and Regulatory Affairs at (202) 442-4311. You can also call Office of the Attorney General's Office of Consumer Protection or check online to see if there are complaints against a particular contractor.

Request written estimates from several contractors. Request a copy of the contractor's personal liability, worker's compensation, and property damage coverage insurance.

Obtain a written contract describing the work to be performed and make sure the contract states that it is the contractor's obligation to get all necessary permits.

Keep a record of all meetings, phone conversations, and payments.

Do not obtain a home equity loan from your contractor unless you have shopped around for a loan first and compared rates and terms. For a list of approved lenders in your area, visit <http://www.hud.gov/ll/code/llslcrit.cfm> or call (800) 225-5342.



Be wary of a contractor who claims to have “leftover” material from another job or who “just happens to be in the neighborhood.”

Do not hire a contractor who only accepts cash.

Avoid paying the full price up front. You can **ask to pay only a deposit** at the beginning of a job and withhold the final payment until the work is completed and passes any required inspection.



BUYING A HOME

Consider working with a reputable buyer's broker who will represent your interests, rather than the seller's interests.

Have the Home Inspected: Do not sign a sales contract unless it states that the sale is contingent on a completed inspection. Use a licensed home inspector to inspect the home.

If the Home Was Recently Renovated: Check with the D.C. Department of Consumer and Regulatory Affairs (DCRA) to make sure all renovations were performed with permits and by licensed professionals. For a list of DCRA-certified construction inspectors, visit DCRA's website at <http://dcra.dc.gov> or call (202) 442-4400.



HEALTH CARE FRAUD

Health Insurance vs. Medical Discount Plans: Health insurance pays for medical bills resulting from a wide range of health care needs, while medical discount plans offer discounts when you purchase specific services and products from participating providers. Watch out for medical discount plans that offer little, if any, real savings.

Medicare Part D: Do not purchase Medicare Part D prescription drug coverage in response to telemarketing calls, emails or texts, door-to-door solicitations, or other face-to-face contacts, unless you have contacted the seller first.

Avoid Being a Victim of Health Care Scams: The government will not call to sign you up for health insurance or to verify your Social Security number or bank account information. Do not provide your personal information to people who call offering to help you get health insurance.

Generic Drugs: To learn more about generic drugs and whether they are the right substitute for your brand name drugs, talk to your doctor.

Contact Lenses: District and federal laws give you the right to obtain your contact lens prescription from your eye doctor so you can buy replacement lenses from whomever you choose.



HEALTH PRODUCTS/WEIGHT LOSS

Alternative Medicine: A product advertised to be “natural” is not necessarily safe or effective. Talk to your doctor to learn more about an advertised product or treatment.

Herbal or Dietary Supplements can be sold without prior approval or testing by any government agency. The FDA may remove a supplement from the market, but usually only after it gets reports of people suffering serious side effects or other evidence that the product may be harmful.

Miracle Cures marketed as cures for cancer, AIDS, arthritis, or other serious conditions often provide little or no benefit, can be expensive, and may not be a good alternative to conventional treatments.

Weight-Loss Products: There are hundreds of products that promise to help you lose weight by “burning” fat. The only proven way to lose weight and keep it off is a sensible diet and exercise.

Wheelchairs and Durable Medical Goods: Before purchasing medical goods, you should always check and see if they come with any warranty. You can also confirm for yourself any claim that the good is covered by Medicare or Medicaid.



HEARING AIDS

Hearing-aid dealers must be licensed by the D.C. Department of Health.

You cannot be fitted with and sold hearing aids unless you have undergone evaluation and testing by an otolaryngologist within the last three years.

You can cancel your purchase of a hearing aid within 30 days of the sale and obtain a refund of the purchase price less an amount up to 5 percent plus the cost of an ear mold.



LIVING TRUSTS/FUNERAL EXPENSES

Living trusts have been marketed aggressively in seminars and through mailings as a way to avoid the cost and time of the probate process (probate is the legal process for transferring property when a person passes away). Companies in the living will and funeral home businesses sometimes pressure consumers into spending unnecessary sums well in advance.

Marketers often exaggerate the time and cost of the probate process. For simple estates with few assets and investments, purchasing a living trust may not be worthwhile, since setting up a trust usually involves more expense than probating a will. And a living trust that is not drafted by an attorney may later cause you legal problems.

Insurance companies and funeral homes often advise consumers to prepay their funeral costs to spare loved ones the burden and to freeze the cost. However, paying for funeral costs in advance can be risky if the funeral home goes out of business. If you cancel, move, or change your plans, you may not receive a full refund.

Check to make sure that your funds are maintained in a separate escrow account, which cannot be used by the funeral home for its own expenses.

Comparison shop! Often you can make reasonably priced funeral arrangements without setting aside large sums of money or prepaying anything.



CHARITY SCAMS

There are many fraudsters who solicit “charitable” donations and use the money primarily to enrich themselves. Avoid charitable solicitations that:

- ⇒ Refuse to provide detailed information about the soliciting organization’s identity, mission, and costs; how a donation will be used; and whether a contribution is tax-deductible. Visit the Internal Revenue Service (IRS) website to find out if an organization is eligible to receive tax-deductible contributions at <http://apps.irs.gov/app/eos>.
- ⇒ Use names that are similar to, but not the same as, the names of better-known, reputable organizations.
- ⇒ Use high-pressure tactics to try to get you to donate immediately.

Ways to protect yourself:

Ask for details about the charity, including its exact name, address, and phone number.

Research the charity online. Contact the Better Business Bureau’s Wise Giving Alliance: <http://give.org>

Do not provide a charity or solicitor with your personal financial information.

Keep a record of all your donations.

Avoid sending cash or wiring money. It’s safer to pay by check or credit card.



SWEEPSTAKES/PRIZE SCAMS

You receive a letter claiming you've won \$5,000, a luxury vacation, or some other prize. More than likely, if there's actually a prize, it isn't worth much at all. Legitimate sweepstakes are free. That means no "taxes," "shipping and handling charges," or "processing fees." It's illegal to require you to pay or buy something to enter a sweepstakes or increase your odds of winning. Furthermore, promoters cannot claim you are a "winner" unless you've actually won a prize.

A "sweepstakes" may be a scam if:

- ⇒ You have to pay to enter, or you have to send money or buy something before your prize can be released.
- ⇒ The company's name sounds like a government agency, such as the fictitious "National Sweepstakes Bureau." No federal or District government agency will contact you asking you to pay money so you can receive a prize.
- ⇒ Your "prize notice" was mailed by bulk rate.
- ⇒ To win, you are required to attend a sales meeting, which usually involves a high-pressure sales pitch.



TIMESHARE AND TRAVEL SCAMS

Y*ou receive a postcard in the mail with an “urgent” message explaining that you are a “winner” entitled to a free trip for two. In most instances, there is no urgency and all that you have “won” is a chance to attend a lengthy high-pressure sales presentation offering you a membership in a vacation club. The membership is very expensive and to claim your free trip you have to meet a series of conditions and pay related fees.*

- Promises of free trips and discounted vacations can be very appealing, but consumers who sign up for vacation or travel clubs or timeshares often don’t get what they were promised or pay more than they had anticipated.
- Check out the company beforehand by calling OAG’s Office of Consumer Protection, the Federal Trade Commission or the Better Business Bureau to see if any complaints have been lodged against the business.
- Don’t be pressured into making an immediate decision with claims of a “one-time” or “limited” offer. Ask to bring any contract home so you have time to review it.
- Most states provide a right to cancel a timeshare or vacation membership club purchase. In the District, you have 15 days to cancel the purchase of a timeshare. However, there is no such similar right to cancel a vacation membership club purchase, so be careful.



CAR PURCHASES

With most car purchases, there is no “cooling-off” period that allows you to change your mind and cancel the purchase, so make sure you consider your choice carefully.

When buying a car from a private seller, in order to register and title the car in the District, you will need:

- ⇒ **Verification of the odometer reading** (recorded on the back of the title or on the inspection certificate).
- ⇒ **A bill of sale** from the seller for your records.
- ⇒ **A vehicle inspection**, if the inspection is not current.
- ⇒ **Auto insurance** coverage for the car.

In deciding whether to **lease a car** instead of purchasing one, you need to consider all of the costs. In addition to the monthly lease payments, there may also be:

- Up-front payments
- Maintenance and repair costs
- Penalties
- End-of-lease costs
- Mileage limits

Is the car you purchased a lemon?

You have purchased a new car and it is having repeated problems that the dealer cannot fix. If you are asking yourself whether the car is a lemon, you need to know the following:



Is the car you purchased a lemon? (cont.)

For a car to be considered a lemon under the District's "Lemon Law," it must experience a defect within two years of the date of purchase or before the vehicle is driven 18,000 miles, whichever event is earlier.

The defect must be subjected to a reasonable number of repair attempts by an authorized dealer and the defect must continue to exist after reasonable attempts at repair. For example:

- ⇒ A non-safety-related problem that continues after four or more attempts to repair.
- ⇒ A safety-related problem that creates a risk of fire, explosion, or is otherwise life-threatening, and continues after one or more attempts to repair.
- ⇒ A vehicle that has been out of service by reason of repair of any defects for a cumulative total of 30 days or more.

When returning a lemon, the dealer must either replace the vehicle or refund your purchase price, less a reasonable amount for your use of the vehicle and damages beyond normal wear and tear.

The Lemon Law does not apply to used cars, motorcycles, motor homes, or recreational vehicles.

Used Cars: Dealers must provide written notice to prospective purchasers of mechanical defects and any known damage to the vehicle due to fire, water, collision, or other causes for which cost of repair exceeded \$1,000.



INVESTMENT SCAMS

If a deal sounds too good to be true, it probably is. An investment opportunity cannot offer both low risk and a high rate of return. Here are some tips:

Independently verify any claims: It is easy for promoters to make exaggerated claims about an investment's profit potential and relative risk. Consult independent sources.

Research before investing: Offers to sell securities must either be registered with the Securities and Exchange Commission (SEC) or qualify for an exemption. To see whether an investment is registered, check the SEC's database at <http://www.sec.gov/edgar/searchedgar/companysearch.html>.

Be skeptical of references: Fraudsters often use false references to reassure people that the claims made for an investment are true. Do your own research rather than relying on references provided by the seller of an investment.

Beware of high-pressure pitches: Don't believe that you are being offered a "once-in-a-lifetime" opportunity. Don't make an investment decision until you have had time to become an informed investor.



FINANCIAL EXPLOITATION

Financial exploitation occurs when an elderly relative's funds or property are used for an illegal or improper purpose. Financial exploitation can take many forms, including scams, abuse by trusted individuals (such as family members or friends), and predatory products and services marketed specifically to the elderly.

Any of these 10 signs may indicate financial exploitation, according to the National Center on Elder Abuse (<https://www.ncea.acl.gov/>):

1. Sudden changes in account balances.
2. Names added to an account.
3. Unauthorized withdrawals from an account.
4. Abrupt changes in a will or financial instrument.
5. Unexplained disappearance of funds or valuables.
6. Substandard care being provided or unpaid bills.
7. Forged signatures in financial transactions.
8. Sudden appearance of previously uninvolved relatives.
9. Unexplained transfers of assets.
10. Provision of services that are not necessary.

(Continued on the next page)



In order to protect a loved one from financial abuse:

Consumer Reports recommends having a family discussion concerning the relative's long-term care. Be sure to include how the caregiver(s) will be compensated.

Check the background and reputation of caregivers.

Accompany elders to meetings with financial advisors. Financial advisors who are paid on commission may "recommend" financial products that may not make sense for your relative.

Just as with health care, regular check-ins on a relative or friend are the best way to prevent problems or at least spot them quickly.

If your relative is having difficulty managing his or her own finances, you may want a trusted person to be given a *Power of Attorney*. This is a document that gives that individual the authority to act for your relative in specified, or all, legal or financial matters.



HELPFUL RESOURCES

Consumer Complaints

Office of the Attorney General for the District of Columbia

(202) 442-9828

Consumer.Protection@dc.gov

<http://oag.dc.gov>

Employment

D.C. Department of Employment Services

Phone: (202) 724-7000

<http://does.dc.gov>

Housing/Licensing

D.C. Department of Consumer and Regulatory Affairs

(202) 442-4400

Regulatory Investigations: (202) 442-8676 (to report a business that is not licensed)

Licenses: (202) 442-4311 (to determine if a business is licensed)

<http://dcra.dc.gov>

Human Rights/Discrimination

D.C. Office of Human Rights

(202) 727-4559

<http://ohr.dc.gov>

Insurance/Securities/Banking

D.C. Department of Insurance, Securities and Banking

(202) 727-8000

<http://disb.dc.gov>



HELPFUL RESOURCES

Landlord/Tenant Issues

D.C. Office of the Tenant Advocate

(202) 719-6560

<http://ota.dc.gov>

Landlord Tenant Resource Center

(202) 508-1710

Utilities (Phone, Gas, Electric)

D.C. Public Service Commission

(202) 626-5100

<http://dcpsc.org>

D.C. Office of the People's Counsel

(202) 727-3071

<http://www.opc-dc.gov>

Consumers Seeking Legal Advice

D.C. BAR Pro Bono Program: (202) 737-4700

Legal Aid Society: (202) 628-1161

Neighborhood Legal Services Program:

(202) 832-6577

The Bar Association of the D.C., D.C. Lawyer Referral Service: (202) 223-6600



NOTES

[illegible]



Connect with the Office of the Attorney General for the District of Columbia

441 4th Street, NW, Washington, DC 20001

Phone: (202) 727-3400 Fax: (202) 347-8922 TTY: (202) 727-3400

Email: Consumer.Protection@dc.gov

CONSUMER HOTLINE — (202) 442-9828

www.oag.dc.gov

STAY CONNECTED



CONSUMER HOTLINE — (202) 442-9828