Nothing is more frustrating than spending your hard-earned money on a product or service only to find that it wasn’t what you thought you were paying for—or that you’ve been scammed. In many cases, simply contacting the business, its manager, or a customer service representative can settle any dispute you may have. But when that doesn’t work or you’re the victim of a scam, my office’s Consumer Protection Division may be able to help.

While attorneys in the Office of the Attorney General cannot represent individuals in lawsuits, our mediation program can assist in resolving disputes or complaints filed by individual consumers. When patterns of fraud, deception or unfair methods of competition emerge, my office may file suit against a business on behalf of all Illinois consumers. That is why it is important to contact us promptly and file a complaint. The sooner we know about questionable business practices or scams, the less likely it is that a fly-by-night operator will leave town or go out of business before consumers can get their money back.

If you feel you have been a victim of consumer fraud, please call one of the helplines listed in this brochure. By working together, we can better protect all Illinoisans from consumer fraud.

HOW TO FILE A CONSUMER COMPLAINT

When submitting a consumer complaint, please supply all information requested on the consumer complaint form, including:
• Your complete address and phone number
• The business’s address and phone number
• Copies of all supporting documentation

The information you submit will be used by attorneys, investigators and other members of the Attorney General’s staff.

If appropriate, we will forward a copy of your complaint to the subject of the complaint. This information also may be shared with other governmental enforcement agencies responsible for consumer protection and other laws.

Complaint forms are public records, which are subject to the Freedom of Information Act. If we receive a request for copies of records that include your complaint, we may be required to provide a copy of your complaint to the requester. However, information that would reveal your identity as a complainant is exempt from disclosure and will be deleted from copies we provide, allowing the requester to read your complaint without compromising your privacy.

Complaint forms may be accessed on our website, IllinoisAttorneyGeneral.gov, or obtained by calling one of the consumer fraud helplines listed on the back of this brochure. You may complete and submit the form online or mail the complaint form and any other relevant documents to:

Office of Illinois Attorney General
Kwame Raoul
Consumer Fraud Bureau
500 S. Second Street
Springfield, Illinois 62701
Or
115 S. LaSalle Street
Chicago, Illinois 60603

CONSUMER FRAUD HELPLINES

CHICAGO
115 S. LaSalle Street
Chicago, Illinois 60603
1-800-386-5438

SPRINGFIELD
500 S. Second Street
Springfield, Illinois 62701
1-800-243-0618

CARBONDALE
1745 Innovation Drive, Suites C & D
Carbondale, IL 62903
1-800-243-0607

HEALTH CARE HELPLINE
1-877-305-5145

SENIOR FRAUD HELPLINE
1-800-243-5377

Individuals with hearing or speech disabilities can reach us by using the 7-1-1 relay service.


Avoid Common Consumer Scams
REAL-TIME IMPOSTER SCAMS

Imposter scammers may pretend to be from a government agency, business, or charity. If they can make you believe them, they can steal your personal information and your money.

For example, scammers call and pose as a "representative" from the IRS or a utility electric company. They may threaten to cut off service or take legal action if you don’t pay.

Sometimes the scam is a story about a family member in trouble. The imposter will “help you” arrange payment for bail, travel, or an emergency. With tricks like artificial Intelligence technology (AI), you may believe your loved is in harm’s way.

What to watch out for...

- High pressure tactics and an urgent need to pay now.
- Demands for wire transfers, gift cards, online payments, or cryptocurrencies.
- Threat of arrest or jail if you don’t pay.
- One imposter scam on the rise is the “sweetheart scam.” The scammer takes romantic interest looking for ways to convince you give him or her money.

What you can do...

Hang up and call the agency, company, or your loved one yourself using a trusted phone number.
- Contact your utility company directly before providing any payment information.
- Do not send money. Wire transfers are like sending cash and can’t be recovered.
- Do not purchase debit cards or gift cards as a form of payment.
- Do not give the caller your financial or other personal information, especially your Social Security or bank account numbers.
- Report the incident to local law enforcement and the Office of the Attorney General.

HOME REPAIR SCAMS

Your home is often your most valuable asset. It is also an easy target for scams. After a weather event, fly-by-night contractors may come knocking with “special” discounts. Sometimes work gets started, but the repairs don’t get finished.

What to watch out for...

- Companies that only have a phone number or PO Box with no physical location.
- A salesperson or contractor offers to inspect your home for free.
- Demands for cash payment or full payment before work is completed.
- Refusal to provide references or proof of insurance when requested.
- Offers of discount prices that seem too good to be true.
- Contracts that include blank spaces.

What you can do...

- Ask people you know for referrals to businesses that did good work for them.
- Refrain from opening your door to contractors or salespeople unless you initiated the call.
- Get at least three written estimates.
- Check the contractor’s background references and prior work.
- Know what licenses are required in your municipality and their rules for solicitation.
- Report scams to local law enforcement and the Office of the Attorney General.
- Complete the Home Repair Know Your Consumer Rights form with the contractor before work starts.
- Contact the Office of the Attorney General, Better Business Bureau, or your local Chamber of Commerce for more information.

CHARITY SCAMS

Not every organization that claims to do good is worthy of a donation. Some organizations will use deceptive techniques and high-pressure tactics to convince you to provide your financial information or cash to make a donation.

Non-profit organizations that solicit donations in Illinois are required to register with the Illinois Attorney General’s Office. If they don’t, that is a sign to take a closer look.

What to watch out for...

- A phony charity that uses a name that sounds like a better-known, reputable organization.
- The solicitor can’t or won’t answer basic questions about the charity.
- High-pressure tactics to make you donate right away.

What you can do...

- Requests to donate using cash instead of a check.
- Find out if the charity is registered with the OAG by calling 312-814-2595 or checking charitableviewer.ilag.gov.
- Ask for the charity’s length of operation, exact name and local and national addresses.
- Ask what percentage of funds raised actually goes to the cause, and request a current financial statement.
- Slow the process down and ask for information to be mailed instead of doing payment on the phone.
- If you feel a solicitation is suspicious, do not donate and report it to the Office of the Attorney General.

ONLINE OR PHONE MARKETING SCAMS

Telephone and online marketing scams are more than annoying. In many cases, the goal is identify theft plus a financial loss. The scams could come as emails, calls, or text messages. The scam artists try to lure you into answering questions or clicking on links to make you give up your personal identifying information.

What to watch out for...

- Offers of tech support because the goal may be to gain remote access to your devices.
- Messages from your “financial institution” asking for sensitive account information.
- A pop-up message or text that directs you to a website to update or verify account information such as PINs or passwords.
- Offers of travel packages, get-rich-quick schemes, special savings on phone service, electricity, or other utilities.
- Notice of a lottery or a “free” gift, vacation or prize, but you must pay for shipping and handling, processing, taxes, or other charges.

What you can do...

- Sign up for the national Do Not Call Registry at donotcall.gov or call 888-382-1222.
- Hang up the phone, and do not answer subsequent calls from the scammer’s number.
- Ignore the email or text, and do not click links inside it. Don’t open attachments if you do not know who sent them or why.
- Refrain from providing personal or financial information to unsolicited calls or messages.
- Report the incident to local law enforcement and the Attorney General.

HEALTH CARE SCAMS

Our health is important and can and be fragile. It’s possible to fall for health care scams that promise “cure-all remedies” or promote a “scientific breakthrough.”

Scammers may offer free medical products or devices. Scammers may also say that they require payment upfront for a product. Similarly, they send a product with the promise that your insurance will cover. However, when insurance denies the claim, the patient is now on the hook for payment.

Medicaid fraud occurs when a Medicaid provider knowingly makes, or causes to be made, a false or misleading statement or representation to obtain reimbursement from the medical assistance program.

What to watch out for...

- A health clinic requires you to travel and stay far from home during treatment.
- A health product is advertised as a scientific breakthrough, miraculous cure, exclusive product, ancient remedy, or a secret ingredient.
- A health product is advertised with impressive, but undocumented, results.
- A promoter tells you there is a conspiracy to suppress the product by health care companies and doctors.

What you can do...

- Ask a pharmacist, doctor, or health professional about the product or service before purchasing or using it.
- Contact the Office of the Attorney General’s Health Care Bureau at 1-877-305-5145 for more information, to report a scam, or to complete an online complaint form.

Text messages that appear to be from official entities (“smishing”) or phone calls made to look like the call is coming from a legitimate or familiar number (“spoofing”). The message may include problematic links.

- A phony charity that uses a name that sounds like a better-known, reputable organization.
- High-pressure tactics to make you donate right away.
- Refrain from providing any payment information.
- Discounts for insurance when requested.
- Offers of tech support because the goal may be to gain remote access to your devices.
- Messages from your “financial institution” asking for sensitive account information.
- Offers of travel packages, get-rich-quick schemes, special savings on phone service, electricity, or other utilities.