



Consumer Protection *for* Wisconsin

Wisconsin Department of Agriculture,
Trade and Consumer Protection

The Wisconsin Department of Agriculture, Trade and Consumer Protection is the state's primary consumer protection agency. Its Bureau of Consumer Protection has authority to regulate unfair business practices. The Bureau receives and responds to thousands of inquiries, and it reviews, examines, and investigates thousands of complaints every year.

This guide summarizes common consumer protection issues facing all Wisconsinites and advises consumers on how to avoid problems – and what to do if a problem occurs. From resolving issues with an auto mechanic or a home improvement contractor to avoiding potential scams and identity theft, the Bureau of Consumer Protection takes great pride in informing, educating, and protecting the public.

What the Bureau of Consumer Protection Does

- ▶ *Regulates unfair and deceptive business practices to protect millions of Wisconsin consumers.*
- ▶ *Provides information, training, and resources for businesses to serve Wisconsin consumers better.*
- ▶ *Administers Wisconsin's telemarketing "Do Not Call" Law.*
- ▶ *Educates consumers on best practices to combat and avoid identity theft, and offers recovery services to identity theft victims.*

Copies of this guide and additional materials about topics within this guide are available from:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison, WI 53708-8911
datcp.wi.gov

Contact Information:

Call our toll-free hotline at (800) 422-7128 or email us at DATCPHotline@wisconsin.gov.

To file a complaint visit our website:

ConsumerProtection.wi.gov.

A digital version of this guide can be found at:

ConsumerGuide.wi.gov

Table of Contents

| | |
|------------------------------------------------|-----------|
| <i>Protection of Your Personal Identity...</i> | <i>1</i> |
| <i>Protection on the Phone and Internet...</i> | <i>3</i> |
| <i>Protection at Home...</i> | <i>13</i> |
| <i>Protecting Your Money...</i> | <i>22</i> |
| <i>Protecting Your Purchases...</i> | <i>30</i> |
| <i>Protecting Job Seekers...</i> | <i>32</i> |
| <i>Protecting Travelers...</i> | <i>34</i> |
| <i>Small Claims Court...</i> | <i>36</i> |
| <i>Additional Resources...</i> | <i>37</i> |

Protection of Your Personal Identity

Identity theft continues to be the fastest growing crime in the country.

Identity thieves can destroy a person's financial reputation and cause endless stress with only a tiny bit of stolen information. Identity theft costs consumers millions of dollars in fraudulent charges each year, and these losses can take years and cost thousands of dollars to recover.

Identity theft and fraudulent scams are here to stay. The rising popularity of the Internet and online purchases enables scammers from around the world to steal our identities and use them for financial gain, criminal activity, and more. The Bureau of Consumer Protection focuses on both prevention and recovery. The Bureau educates consumers on how to monitor and safeguard personal information to keep it safe from thieves. It also works with victims of identity theft to help them reclaim their identity and restore their credit standing.

Four Tips to Protect Yourself From ID Theft

- ▶ *Do not give your personal information to anyone you do not know or trust.*
- ▶ *Ask questions before you share any personal information. Why is it being requested? How will it be used? By whom?*
- ▶ *Store your personal information securely. Never store sensitive data on computers, phones, or tablets.*
- ▶ *Use antivirus and antimalware programs to protect your devices. Be wary of emails, texts, and calls that sound suspicious, include unknown links, or request immediate action from you.*

If you are a victim of identity theft or a similar scam, report it to local law enforcement, tell your bank and credit card companies, and file a complaint with the Bureau of Consumer Protection. In addition, report the identity theft to all three credit reporting agencies to place a security freeze on your credit reports. The freeze costs nothing, and it allows you to prevent accounts, loans or new credit cards from being approved without your consent. These steps are critical to take back your identity.

To place a freeze, contact all three credit reporting agencies individually:

Experian

experian.com/freeze

Equifax

equifax.com/personal/credit-report-services/credit-freeze/

TransUnion

transunion.com/credit-freeze

Identity theft is an ongoing crime.

Continue to read your credit card statements, credit reports, and Social Security earnings statements.



Protection on the Phone and Internet

Phone and Internet providers typically offer a variety of services, often bundled into packages. Bundling can save money on your overall bill, but it can also lock you into receiving unnecessary services or ones you cannot easily cancel.

Read the Contract Before You Sign It!

Check your phone or Internet contract for:

- ▶ *A clear description of the service and its feature.*
- ▶ *The price you will pay for the service.*
- ▶ *Any incidental charges, including connection or disconnection fees.*

Purchasing Tips

- Find out what phone, video, and Internet service provider options are available in your area.
- Check for discounts available to new subscribers or for purchasing a package of bundled services.
- Get information in writing about early termination fees for disconnection of service – especially if you decide to drop one component of a bundled service.
- Get the return policy and all other details in writing.
- Immediately after you receive a telephone, test it where you intend to use it most. If it does not perform as advertised, take it back.

Cramming

Cramming is when companies add charges to your telephone, Internet, or credit card bill for extras you never approved, such as voicemail, web design, Internet access, or club memberships. Cramming charges can be easy to overlook. Often, cramming occurs after you fill out a contest entry form, coupon, or other sign-ups. These documents may have very fine print that includes an agreement to buy a service that will be charged to your telephone number or credit card bill. Other times, cramming may occur when you agree to switch service providers.

How to prevent cramming

- Look at junk mail carefully. It could be a negative option notice saying that you will be charged for a service unless you contact the company to cancel it.
- Do not call back numbers or reply to emails that you do not recognize. A crammer may see your number and process an unauthorized request for service.
- Be cautious of websites that ask for your phone number. Entering a phone number to get a “free offer” may result in other services being added to your phone bill.

Wisconsin Do Not Call Registry

Getting your landline and cell phone numbers on the Wisconsin Do Not Call Registry is free and available to all residential phone customers in Wisconsin. Register at DoNotCall.gov or (888) 382-1222. You must call from the telephone number you wish to register.

The Wisconsin Do Not Call list helps reduce (not stop) unsolicited telemarketing calls and text messages. While being on the list does not stop illegal scam calls, it helps consumers identify scammers from legitimate business that follow the law. It is important to report businesses that call to solicit goods and services if you are on the list so DATCP can enforce the law.

Exemptions

Exemptions from Do Not Call rules include:

- ▶ *Calls to current clients.*
- ▶ *Calls from non-profits seeking donations.*
- ▶ *Calls made for polls, surveys, and political purposes.*
- ▶ *A call made by an individual acting on their own behalf and not as an employee or agent for any other person.*

Read your bill every month.

Check for charges of services you did not request.



Robocalls

Robocalls may include a message that claims to offer a lower credit card rate, extend your car's warranty, eliminate your student loans, lower mortgage interest rates, provide information about home security systems, provide "free" medical equipment or health care discount plans, or any other variety of alarming notices and too-good-to-be-true offers. Robocalls may include a message from "Rachel," "Card Holder Services," or something similar – and can sound like real people leaving a legitimate message.

Because most illegal robocalls come from foreign countries that do not cooperate to stop the criminal behavior, consumers should protect themselves.

Common Telephone Imposter Scams

- **Social Security Administration (SSA).** These are threatening calls about supposed problems with your Social Security number. The real SSA will not contact you, out of the blue, to verify your Social Security number, to wire money, or to put money on a gift card.
- **IRS or US Treasury.** These are threatening calls that say you must pay now for tax violations or be arrested, sued, or deported. The real IRS will not contact you by phone. They will not make threats.
- **Utility shut off.** These are threatening calls that state you have not paid your utility bill and someone is on the way to disconnect your service unless you pay immediately.
- **Law enforcement.** These are threatening calls that state there is a warrant for your arrest or you failed to appear for jury duty. The caller demands you pay immediately to avoid prosecution or jail time.
- **Friend & Family Scam.** A caller pretends to be your family member or friend and begs you to send money immediately and to keep the situation a secret from other relatives. The money may be to get out of jail, to pay for a car repair, to get home from a foreign country, or to pay for an emergency room or hospital visit.

Protect yourself from phone scammers

- Beware of callers who ask you to send money by gift card or money transfer (Western Union, MoneyGram, Venmo, Zelle, or prepaid card) or to buy something without letting you verify its authenticity.
- Never give out your credit card, Social Security number, or bank account numbers or any other personal or sensitive information to someone you do not know.
- Never pay anything for a “free prize.”
- Do not rush into anything.
- If a caller offers to send a messenger to your home to pick up your payment, end the call.

Do Your Research!

- ▶ *Check with the Bureau of Consumer Protection and the Better Business Bureau.*
- ▶ *Confirm the seller’s physical address and phone number.*
- ▶ *Be careful about overseas businesses. You may not have the same protections or be able to enforce your rights as easily.*
- ▶ *Search the company name online with terms like “scam”, or “review” to find out what others are saying.*

Spooﬁng

Scammers have the ability to block their real identities from showing up on your caller ID, email, or text messages. This is called spooﬁng. The scammer may appear to be a friend, official website, or a trusted source with whom you feel comfortable.

Online Security

What is malware? *Malware is any program designed to cause harm to your device, like a computer virus. It’s short for “malicious software.” Use reputable antivirus and antimalware services to defend your data from cybercrime.*

Online shopping allows consumers to purchase practically anything quickly and easily. However, the Internet has many fake ads, fraudulent websites, and scammers trying to take your money and give you nothing in return. You can have a safe online shopping experience as long as you protect yourself.

Your best protection when shopping is to do business with familiar companies. No matter how impressive a company's website is, how convincing a telemarketer sounds, or how sincere a door-to-door salesperson may appear, if you are not familiar with a company's reputation, check it out.

Tips

- ▶ *Use virus protection, spyware protection, firewalls, or other filtering software and keep it updated.*
- ▶ *Use strong passwords and keep them updated. Use different passwords for all your accounts.*
- ▶ *Delete messages from people you don't know without opening or responding to the messages.*

Phishing

Phishing (pronounced "fishing") is when scammers try to trick you into giving up your personal or confidential information like usernames, passwords, and credit card details through email or fake websites, so they can steal your identity or hack into your accounts.

Avoid phishing scams

- Don't respond to emails and letters that claim your bank account will be charged for an unfamiliar subscription.
- Don't call the phone numbers listed on suspicious letters received via email, text, or mail.
- Don't click on pop-ups that appear on your computer.
- Don't give out personal information such as date of birth, Social Security Number, credit card numbers, or bank account numbers.
- Never allow remote access to your computer unless it is a trusted source.
- Never give out your passwords or any confirmation codes to a stranger over a text, email, or phone call.

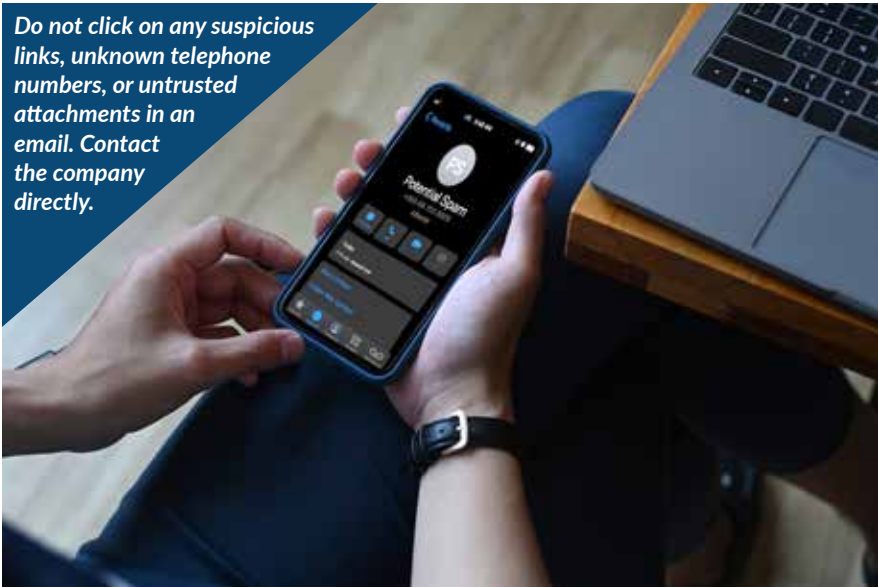
Shipping notices

Scammers may send you fake shipping notices via email or text that look like they are from a legitimate shipper like UPS, FedEx or Amazon. They claim that you have a package waiting or there is a problem with a delivery or order. They ask you to open an attachment for the shipping/invoicing details or to click a link to review your account. They are really phishing for your personal information, hoping you'll give it to them voluntarily or that you'll unknowingly download malware which can scan your device for sensitive data without your knowledge.

Renewal notices

Fake renewal notices sent via email, text, or mail, may claim your subscription to a product has been renewed and your bank account will be charged several hundred dollars. The letters often give you a phony customer service number that connects you to a scammer waiting to take your personal information.

Do not click on any suspicious links, unknown telephone numbers, or untrusted attachments in an email. Contact the company directly.



QR codes

QR codes are square graphics that work similarly to bar codes and can be scanned by your phone's or smart device's camera to activate apps, track packages, or view menus right on your device. But because these codes can't be read by the human eye, they have become a common way for scammers to disguise malicious links. Scammers can use this technology to lure you to a phishing website where you are directed to enter personal, account, or financial information, or even force malware downloads onto your device without your permission.

When Using QR Codes

- ▶ *Take a close look at the web address before entering any information to ensure it is not an imposter account.*
- ▶ *Be wary of shortened website links. If a shortened link appears when you scan a QR code, it could be disguising a malicious website address that you'll be redirected to if you open the page.*
- ▶ *Watch out for signs or flyers that show signs of tampering. Some scammers attempt to mislead consumers by altering legitimate business ads by placing QR code stickers over the real QR code.*
- ▶ *Install a QR scanner with added security. Some antivirus companies have QR scanner apps that check the safety of a scanned link before you open it. They can identify phishing scams, forced app downloads, and other dangerous links.*



Mobile Device Apps

While many apps are available to download for free, many free apps also offer opportunities to make purchases after you download. These in-app purchases may provide additional features or content, like recurring subscriptions, an ad-free experience, a 'pro' version of the app, in-game currency, extra game levels, or other unlockable features. Some risks are associated with in-app purchases.

Benefits of In-App Purchases

- ▶ *Quick and seamless transactions.*
- ▶ *New content and features available immediately.*
- ▶ *You can control in-app purchasing.*

Children can spend money without realizing.

Children using their parent's devices may not realize that in-app purchases are spending their parent's money.

It is easy for you to spend a lot of money without realizing.

You can spend money within a game or app without realizing it because you don't have to submit credit card details with each transaction. Small purchases can add up quickly.

Unencrypted data isn't secure.

Apps may collect data such as name, email address, phone number, home address and credit card info and leave it unencrypted, making it easy for scammers to steal.

Location data may be shared or sold without your knowledge.

Some apps, like maps or weather apps, need to know your location to function. However, many apps want this data for advertisers, who pay app developers a lot of money to know your location so they can target you with specific ads. Apps that want your location data must get your permission, which can be turned on or off at any time in your app settings.

Logging in through third-party apps puts your data at risk.

Logging into your personal accounts directly instead of allowing other apps to log-in for you can help prevent your information from being shared unintentionally.

Online Scams

The ability to become anonymous on the Internet means most websites, even common social media platforms like Facebook and LinkedIn, can be used by scammers to find victims.

Pet scams

If you are looking to buy a pet, you should be careful about buying one online. Scammers pretending to sell pets will create fake websites and often post photos of “their” animals online. They may even look like they are in your area. However, after you pay them, the scammer may claim to need more money for transport fees, licenses, or permits. Once you realize what is happening, it may be too late. The website might be gone, and the scammer can no longer be contacted.

Before you buy a pet, ask for the name and location of their veterinarian. If the seller provides this information, search for the veterinarian online and contact their office. Don't use a phone number the seller gives you; look it up yourself. A list of licensed Wisconsin veterinarians is available on our website at datcp.wi.gov.

Be wary of offers that are urgent or too good to be true. Do not pay upfront.



Romance scams

Social media, dating websites and apps, and online personal ads are romance scammers' go-to tools for finding victims. Scammers create phony profiles that often involve the use of a stranger's photos they found online. They use these profiles to gain trust and love from a victim and convince them to send money for travel expenses, legal help, medical bills, or any number of other made-up issues.

If you are communicating with someone using an online dating tool, ask questions, look for inconsistent answers, and take it slow.

Signs of a Romance Scam

- ▶ *They claim to be from the United States but are currently "traveling," "deployed with the military," or "working overseas."*
- ▶ *They profess love for you almost instantly.*
- ▶ *An online reverse image search of the photo reveals they are impersonating another individual.*
- ▶ *They ask you to leave the dating site and communicate by email or instant messages (i.e. Google Hangout, WhatsApp, etc.).*
- ▶ *They ask you for personal information including Social Security, bank account, or credit card numbers.*
- ▶ *They ask you to cash checks, send money by wire transfer, invest in cryptocurrency, or purchase and send them pre-paid cards.*
- ▶ *They make excuses for not meeting in person.*



Protection at Home

Finding and maintaining a home can be stressful. Housing is one of every person's most basic needs, and the market can be difficult to navigate. Homeowners and renters both have rights and obligations, and should know how to protect themselves and their property.

Landlord/Tenant

Consumer protection laws help ensure that residential rental agreements are fair, potential renters are informed of existing laws before entering a rental agreement, and former tenants are protected when they move out. Renters can protect themselves in all three phases of renting.

Early considerations

Before moving in, inspect the property for possible issues affecting habitability. The landlord must disclose uncorrected code violations if the landlord knows about them and they are a threat to your health or safety. In addition, if the unit's plumbing is not in good operating condition, or the unit's heating is incapable of maintaining a temperature of at least 67 degrees, or the unit's electrical wiring is not in safe operating condition, the landlord must disclose such conditions even if the landlord has not received notice of a code violation.

If charges for water, heat and electricity are not included in the rent, understand how utility payments will be split. If utilities are not included in the rent, and the unit is not separately metered, then the landlord must clearly disclose those facts and explain how the charges for utilities will be determined.

Renting tips

If you pay a security deposit, always complete the check-in sheet and return it to the landlord within seven days after the start of tenancy. Keep a copy for your records.

Make sure you know who to contact regarding maintenance problems. This might be the owner or a third-party service.

You will usually be responsible for routine minor repairs. However, the landlord is responsible for making repairs necessary to keep the premises safe. If the landlord refuses to repair major building defects, you may report the defect to your local building or health inspector. By law, the landlord may not retaliate by evicting you.

You must give access to your landlord to inspect, repair, or show your unit at reasonable times. The landlord is required to give you at least 12 hours' notice to enter, unless it is an emergency or you agree to something else.

If your rental agreement is a lease for a term, like six months or a year, you must move out at the end of the term, unless you sign a new rental agreement or the landlord accepts rent for the next month. If the landlord continues to accept rent past the end of the lease term, and if a new rental agreement has not been signed, you are now in a month-to-month periodic tenancy by operation of law. In such a month-to-month periodic tenancy, most provisions from the term lease still apply.

Move-out tips

If you move out at the end of your lease, the landlord must return your security deposit within 21 days. If you move out before the end of your lease, the landlord has 21 days to return your security deposit from either the last day of your lease or the date a new tenant moves in, whichever comes first.

The landlord may deduct from your security deposit for unpaid rent or damage caused by you or your guests.

If there are any deductions from the security deposit, the landlord must give you a written itemized statement.

The cost of addressing normal wear and tear, such as routine carpet cleaning may not be withheld from your security deposit or collected by the landlord in advance.

Senior Living/Housing

An increasing number of private businesses offer senior housing for those who do not need or want to move into an assisted living environment. With senior housing, buyers may purchase an individual unit and pay annual maintenance fees.

In some cases, the businesses will agree in advance to repurchase back or resell the unit if the owner moves or passes away.

Before signing or investing

Take your time and read through the contract thoroughly, ask questions, and fully understand the written details of the contract offer.

Have a friend, loved one, or other third party (possibly an attorney) offer a second opinion on the contract offer.

Find out if the Bureau of Consumer Protection and the Better Business Bureau have complaints against the company you are considering.

If a money-back or buy-back guarantee is offered...

- Know whether the refund is dependent upon the sale of your unit, and what happens if other comparable units are for sale at the same time.
- Know what percentage of your original investment will be returned to you.
- Get written details on how you will get the money for a future buy back.

Manufactured Homes

Manufactured homes, sometimes referred to as “mobile” homes, are houses built in a factory and later transported to a lot rather than being constructed on-site. This building method is faster and cheaper than traditional home construction. Many people think of “mobile” homes as large trailers or recreational vehicles (RVs), but most modern manufactured homes are nearly indistinguishable from a traditional site-built home. Manufactured homes are the only form of housing subject to federal building codes, ensuring customers receive domiciles that are safe, durable, and quality.

Buying

Manufactured homes are cheaper than traditional houses, but buyers will need to account for both the cost of the home and the cost of the site it will be located on. Take your time shopping around to find a convenient site where the value of the land or home won't diminish over time. These sites can be owned or rented.

If you plan on living in a manufactured home community, closing on a manufactured home purchase should not occur until after the buyer's application for tenancy has been approved by the community operator.

A community operator can't charge you a fee to enter or exit a manufactured home community.

Leases and Protections

Community operators must offer tenants a lease for no less than one year and should provide a written copy of their lease.

Tenants are protected against rent increases and other changes during the entire term of their lease.

If they are terminating or not renewing a lease, community operators must provide the tenant with a written notice explaining the reason why.

Selling

Tenants have a legal right to sell their homes and leave them in place in the community if the home's condition meets the community's reasonable standards and the buyer's credit application is approved.

Some leases require that a tenant selling their home must inform the landlord in writing prior to the intended closing date. Some operators require that homes pass an inspection prior to considering a prospective buyer's application for tenancy. After inspections, it is important that the seller accompany the buyer to the operator's office to request an application for tenancy.

A tenant can't be required to make their community operator their sales agent too. Operators can't receive anything in payment for transferring tenancy from a home seller to a buyer.

Read your lease carefully and keep a copy in a secure location to refer to when needed.



Home Improvement

A contractor's quality of work can be frustrating if a project is not done to a consumer's satisfaction. When selecting a contractor, consider the following:

- Try to hire a local contractor to do the repairs, especially if your area was recently hit by a storm or natural disaster.
- Get two or three cost estimates in writing before choosing a contractor.
- Get references on the contractor and contact them.
- Ask whether the contractor will be subcontracting your job, and if so, who will perform the work.
- Get all estimates, contracts, and warranty information in writing, including a start and completion date, exactly what work is to be done, and what materials will be used.
- If you have a three-day right to cancel, get two copies of the cancellation forms from the contractor.
- Beware of contractors promising to pay or rebate portions of an insurance deductible. If the insurer denies the claim you may be able to cancel the written contract within three days of the notice.
- Request lien waivers from anyone you pay for home repairs.
- Never pay with cash or checks made out to cash.
- Contact the Bureau of Consumer Protection and the Better Business Bureau to check if any complaints have been filed against a contractor or company.



Transient Crews

Transient crews can show up in the wake of major storms or in summer months offering great deals on construction, repair work, windows, asphalt, home alarms, etc. Some may pressure homeowners for upfront payments or increase prices as they work. While many of these crews provide quality, ethical services, some come and go from an area without a trace, leaving consumers empty-handed and with no recourse for unfinished work or damage to the homeowner's property.

Protect Yourself

- ▶ *Check the contractor's credentials by looking up the company's phone number online and calling to verify the identity of the seller.*
- ▶ *Contact the municipal clerk to verify the crew is approved to solicit work in the area.*
- ▶ *Call the police immediately if they do not leave when asked, or if they begin repair work without your authorization.*
- ▶ *Contact the Bureau of Consumer Protection to check if the company has had complaints filed against them.*
- ▶ *Get all agreements in writing and take all the steps you would take if the work was planned ahead of time.*

**Do not let
strangers
into your
home!**



Solar Panels

Solar photovoltaic (PV) system installations are becoming more common in residential areas. Solar energy is an environmentally friendly way to possibly save money on your home's electric bills.

Is solar power right for you?

If you're thinking about using solar power in your home:

- Review your utility bill to see how much electricity you used in the last year and what it cost.
- Evaluate how you use energy. There may be other ways to conserve energy and save.
- Consider your roof. If it needs to be replaced soon, taking the solar panels down will be an additional cost.
- Figure out what size system you need to meet your average energy usage. Calculators from the U.S. Department of Energy are available online.
- Research if your electric utility has rules and policies in place for homeowners who produce solar power. Some may offer money or credit for extra electricity your panels produce.
- Verify if your local government or homeowners association has extra rules or requirements before you buy.

Solar providers and taxes

If a solar company tells you that you'll receive a tax credit or other form of payment from the government or utility companies, have them show you documentation and research it yourself.

Note the Federal Investment Tax Credit for homeowners is a tax credit and not a deduction. If you will not owe federal taxes, or you pay less taxes than the credit amount, then you may not see tax credit savings.

Questions to Ask

- ▶ *What is the total cost and down payment?*
- ▶ *How much will I pay per month for the lease and will it increase?*
- ▶ *If there are any incentives, who receives the incentive?*
- ▶ *If permits are required, who will get them?*

Door to Door Sales

Businesses often engage in door-to-door sales to entice consumers into buying their products or services. Door-to-door salespeople can only sell from 9:00 a.m. to 9:00 p.m. Some cities require them to have a registration stamp before selling door-to-door. Fundraising sales by nonprofit groups are exempt from state door-to-door sales rules, but local laws and ordinances may still apply.

Get all promises and details of agreement offers in writing and request two copies of any cancellation form.

Junk Mail

Scammers can use junk mail to commit financial fraud and even identity theft. Often, the victim doesn't realize it until after their credit is damaged.

Beware: Junk mail may contain scams! Protect yourself by reducing the amount of postal and electronic junk mail you receive.

If you receive mail offers in someone else's name, return them to sender. If the mail offer is addressed to you and you do not want it, shred it.

You can reduce your junk mail

You can eliminate your name from the large mailing lists sold to direct mail marketers by registering with DMAchoice at DMAchoice.org or by calling (212) 768-7277 ext. 1888. You can also opt out of unsolicited credit card offers by visiting OptOutPrescreen.com or by calling (888)-567-8688 and selecting opt-out.



Mail Orders

Ordering merchandise from home can be easy and convenient. When a consumer in Wisconsin receives an advertisement and then orders a product for delivery, the seller must follow certain rules. The seller must ship prepaid merchandise or make a full refund within the delivery time shown on the original order form or advertisement, or within 30 days if no delivery time is stated. The seller may extend the delivery date by sending you a notice stating that it cannot send the merchandise within the original delivery period.

If the seller wants to extend the delivery time, you can:

- Contact the seller and cancel the order. They must give you a refund right away, or
- Contact the seller and agree to a delayed delivery date, or
- Do nothing. The seller must then ship or refund payment within the extended delivery time stated, but can't wait more than 30 days after the original delivery period to do so.

Unsolicited merchandise

Under Wisconsin law, when a seller sends you something you did not buy, it is considered a gift and may be kept without any obligation to the sender. Do not be pressured by any business that mails you unordered merchandise on a "trial basis," and then sends phony invoices trying to get you to pay.

Brushing scams

Brushing is a scam to create fake sales and reviews for a product. Sellers will mail unordered items to individuals and use the recipients' names to post positive online reviews for the product. Scammers hope that the reviews drive additional sales. You are not required to keep or send back anything you receive from a brushing scam; however you may want to report the suspicious unordered items to the Bureau of Consumer Protection. Conduct a search and see if someone has posted a fake review using your name/information/identity as part of the scam.

Protecting Your Money

Without money, there isn't much a person can do or acquire. Consumers need to know how to make, spend, and save money safely, especially online. Scammers and fraudsters would be happy to take it off your hands.

Medical Billing

If you have trouble understanding your medical bills, you are not alone. If you have questions about a bill, contact the hospital or clinic first.

Paying your bill

You are responsible for paying your medical bills. Even if you have medical insurance, it is common for hospitals and clinics to expect you to pay the bill in full immediately after receiving services, rather than billing the insurance company for its share.

If you are uninsured or using a medical service outside of your insurance's network, the medical service provider must give you a good-faith estimate of costs. In certain circumstances, such as when the actual charges are much higher than the estimated costs, there is also a federal dispute resolution process available for individuals who are uninsured.

If you cannot pay your bill

Many hospitals and clinics will offer monthly payment plans. Review the paperwork for the monthly payment plan carefully. Your hospital or provider may be willing to accept smaller monthly payments or be willing to negotiate a payment plan.

Carefully review all medical bills you receive.

Be sure to review bills for errors.



Medical billing tips

Alert your hospital or insurance company of any questionable billings or unpaid balances as soon as possible. Keep a treatment list. Create a log of every test, treatment, and medication you receive.

Watch for statements that state your medical bills were sent to another source for payment.

If you have difficulty understanding the charges on your summarized bill, request an itemized bill.

Charitable Solicitations

Non-profit and charitable organizations may contact you asking for donations. Organizations sometimes pay telemarketers to conduct professional fundraising for them. In some cases, telemarketers keep a large percentage of the donations.

How to be a smart donor

- ▶ *Be wary of groups sending you free gifts to solicit donations.*
- ▶ *You may wish to avoid charities or organizations that do not disclose how much of the money collected is used for charity and how much is spent on salaries and administration.*
- ▶ *Some questionable charities try to fool people by having names, logos, and websites that are very similar to those of legitimate, well-known charities.*
- ▶ *Watch out for fake fundraising schemes that pop up after natural disasters or other tragedies.*
- ▶ *Donate to charities that you trust and are well-established. Start your research at charitynavigator.org or give.org.*
- ▶ *Make sure the charity is registered with the Wisconsin Department of Financial Institutions by calling (608) 267-1711 or checking online at wdfi.org.*



Do research before you give!

Only donate to organizations you know and trust.

Crowdfunding

Crowdfunding sites, like GoFundMe, allow people to raise funds directly from the donations of others. They are easy to set up and the organizer receives the funds quickly; however, not all fundraisers are legitimate.

Things to know

- The campaign organizer sets the fundraising goals.
- Each crowdfunding site has its own set of rules and may charge fees. You should review them before donating.
- The money raised goes to the campaign organizer, not directly to the person or cause it is set up to help.
- Only donations to a charity are tax deductible.

Avoid Scams

- ▶ Find out who is behind the crowdfunding request.
- ▶ Do reverse image searches of any photos used.
- ▶ Donate to campaigns organized by people you know and trust.
- ▶ Research the creator's background and reviews.
- ▶ Has the creator engaged in previous campaigns? How did those campaigns turn out?

Gift Cards

Gift cards work like gift certificates. Losing a gift card is the same as losing cash. Beware that gift cards may not be honored if a company goes out of business. Most importantly, **never** pay for a service or product when the seller requires you to pay using only a gift card - they are trying to scam you!

The federal government regulates the sale of gift cards under Federal Reserve rules (12 CFR § 205.20).

Gift card rules and regulations

On most cards, expiration dates must be clearly stated and extend at least five years after you purchase them. If you can add money to a gift card, the five year expiration date is renewed from the day you added money.

Reward or promotional gift cards for making a purchase can expire in one year.

Dormancy, inactivity, and service fees are allowed when a card has not been used for more than one year.

Rebates

There are no Wisconsin laws that specifically regulate rebate policies. As long as the goods are not misrepresented, each business may set its own rebate policy.

What Can Businesses Do?

- ▶ They can issue rebate refunds in cash, coupons, free products, or free services.
- ▶ They can set specific expiration dates, proof-of-purchase requirements, per-household limits, and other restrictions.

Thinking about rebates

When you request a rebate, follow the requirements carefully.

Think about the true value of the rebate, especially if you are offered in-store credit rather than money back.

Keep copies of rebate forms and write down when you mailed the rebate.

Financial Investing

Financial investment seminars are a way for consumers to learn how to invest their money. However, some seminars may use high pressure tactics to convince you to make investments that may not be right for you. Do not feel obligated to act or invest before you're ready.

If you attend a seminar

Take your time and do not be rushed into buying on the spot.

Investigate any business in which you may invest.

Be cautious of seminar representatives who can't answer questions or don't give straight answers.

Get the investment qualifications (i.e. minimum investment amount) and the company's refund policy in writing.

Get all the details of an offer in writing.



Be on guard against financial investment scams and fraudulent financial advisors.

Tips before investing

Contact the Wisconsin Department of Financial Institutions at (800) 472-4325 or online at wdfi.org, the Better Business Bureau, and the Bureau of Consumer Protection to find out if the company has any complaints filed against them.

Cryptocurrency

Cryptocurrency is a computer-based digital asset that works as a monetary system. Records of who owns “crypto,” in what quantities, and with whom they trade are stored in a ledger called a blockchain created and maintained by networks of computers. There is no centralized cryptocurrency database or guarantor.

What’s an NFT?

Non-fungible tokens (NFTs) are not cryptocurrency, but function in similar ways and are based on the same blockchain technology. *Despite what some users say, they are also prone to scams and fraud.*

A growing number of companies offer Cryptocurrency Deposit Accounts with a simple promise to pay high interest rates. However, investors should know cryptocurrency transfers may be untraceable and irreversible, making users a target for scammers. Cryptocurrency Deposit Accounts, unlike traditional savings accounts, come with big risks.

Cryptocurrency fraud and scams have resulted in individual losses of millions of dollars.

There is little to no regulation around cryptocurrency. Use with caution.

What can you do to protect yourself from cryptocurrency-related scams?

Be aware of SIM card swapping. A SIM (Subscriber Identity Module) card is a small chip that stores information about the device and its user, usually found in cell phones. Hackers can use your stolen personal information to remotely initiate a “SIM swap,” and wipe your cryptocurrency accounts clean.

Be wary of guarantees and big promises. Scammers may offer you free money paid in cash or cryptocurrency and never deliver, or encourage investment in a new coin that they plan to shut down soon after, taking your money with them.

Because cryptocurrency is such a new technology, it is common for new scam methods to develop and spread quickly. It can take

advanced technical knowledge to fully understand how these scams work. Be extra careful.

Because there is no central authority controlling the supply of cryptocurrency, scam victims usually have no recourse and their losses are permanent. Be very cautious when investing, especially with large sums of money.

Research all investments before making any financial decisions. DFI encourages investors to do their homework, ask questions, and contact DFI's Division of Securities at (608) 266-2139 or email DFISecurities@dfi.wisconsin.gov.

Payment Apps

Mobile payment apps such as Venmo, Cash App or Zelle let you send and receive money using your smartphone, making the transfer of money quick and convenient. By adding your bank account and/or payment card to a mobile payment app, you can pay for goods or services with your phone with little delay. Mobile payment apps are more popular than ever, and scammers realize that.

Scammers try to pressure consumers into making quick decisions without doing proper research. They may offer deals that are too good to be true, or list rare items like collectibles or heavily discounted event tickets, or promise large returns on investment. Take time to research sellers before you ever send any money. Be skeptical of suspicious advertisements, offers, and requests.

Send and receive money only to/from trusted sources. Use a credit card for transactions when possible – losses are typically more recoverable than from mobile payment apps or other peer-to-peer payment methods, which usually do not offer the same purchase protection as debit or credit cards.

When Using Online Marketplaces

- ▶ *Verify the seller's identity.*
- ▶ *Read reviews from other purchasers.*
- ▶ *Research their profile.*

Money Scams

Whether it claims to be for a contest, lottery, sweepstakes, or prize promotion, scammers send an authentic looking check, cashier's check, or money order to be deposited into your bank account. Scammers request that you send back a portion of the money for shipping, taxes, processing fees, or other reasons. They are trying to trick you into sending them your real money by offering large sums of bogus money.

Fake check scams

There are many variations of the fake check scam. Scammers often claim to be in another country and say it is too difficult or complicated to send you money directly from their country, so they will arrange for someone in the United States to send you a check. Sometimes scammers pose as American businesses or even government entities. These checks are fake but can look very real – even bank tellers may be fooled.

Although you can withdraw the deposited money quickly, it may take weeks for the forgery to be discovered and the check to bounce. By that time, the scammers have your money, and you owe the bank for the withdrawn money and bounced check fees.



Check overpayment scam

Scammers will intentionally overpay for purchases and act like it was an honest mistake, and then ask you to return the overpaid amount. By the time their check bounces, the scammers will have your refund and maybe even the purchased item too.

Phony and misleading sweepstakes

Scammers will say you won a prize, then ask you to send money or buy something to redeem it. Often, the prize isn't what it seems or doesn't exist at all. Sometimes, magazine sellers offer legitimate sweepstakes as a way to attract new customers. You don't need to make a purchase to enter a sweepstakes and you will have the same chance of winning.

Inheritance scams

Scammers are savvy at convincing people they have inherited a large sum of money and will contact you to get your bank account information so they can send you the money. You will be told to act immediately and that you have to pay taxes or fees. However, there is no money coming to you, and the scammers walk away with your bank information and your cash.

International lotteries

In the United States, it is illegal to use the mail or telephone to play lotteries across national borders or state lines. By responding back to the scammer, you are breaking federal law per *18 U.S. Code § 1953*. Do not reply in any way.

Don't get caught in a money scam!

If a person or entity requests that you wire them money, it is a scam and you will not get your money back! Stop the payment and end communication. Never agree to pay to claim a prize or a gift. Never agree to pay for grants from the government or foundations. Never agree to cash checks and send the money somewhere, especially if it's part of a work-from-home scheme. Do not enter foreign lotteries. If selling a product, do not accept a check for more than your selling price, no matter how tempting. Resist any high pressure tactic to "act now."

Know that just because funds from depositing these bogus checks are available for withdrawal, that doesn't mean the check has cleared. Do not deposit it—report it! Contact the Bureau of Consumer Protection to report all fake check and money scams.

Protecting Your Purchases

A number of laws and private company policies govern how purchases can be made and what obligations buyers and sellers have to each other. Consumers can protect themselves by knowing what information to seek out about potential purchases.

Motor Vehicle Repairs

The best way to avoid motor vehicle repair rip-offs is to be prepared. Knowing how your vehicle works and how to identify common problems is a good start. It is also important to know how to select a good technician/mechanic, what questions to ask, and your consumer rights.

Choosing a repair shop

- Look for an auto repair shop before you need one to avoid being rushed into a last-minute decision.
- Shop around for the best deal and compare warranty policies on repairs.
- Make sure the shop will honor your vehicle's warranty.
- Look for shops that display certifications showing they have a certain level of repair knowledge and abilities.
- Ask if the shop has experience working on your vehicle's make and model.
- Contact the Bureau of Consumer Protection to see if there is a record of complaints about a specific repair shop.

Repair charges

- ▶ *Wisconsin car repair shops must get your authorization for any repair and must offer you an estimate, or firm price quote, if repairs will cost \$50 or more.*

After the work is complete

The shop must provide you an invoice describing the work done. The invoice should list each repair, any parts replaced, and the cost of each part; labor charges, the odometer reading when you brought the vehicle in and the date the vehicle was returned to you.

The shop must also return damaged parts if you requested them before the repairs began. If the shop needs to return a part under

a warranty, the shop must allow you to inspect the parts before your vehicle is returned.

There is no “standard warranty” on auto repairs. Make sure you understand what is covered by your specific warranty. Be aware that warranties may be subject to limitations, including time, mileage, deductibles, businesses authorized to perform warranty work, or special procedures required for coverage.

There can be big differences between the warranties of similar products manufactured by different companies. Federal law does not require manufacturers to issue warranties. If a warranty is offered, it must be easy to read and understand. Every term and condition must be in writing.

Warranties

- ▶ *Full warranties typically cover defective products by fixing or replacing them free of charge and within a reasonable time.*
- ▶ *Limited warranties typically cover parts but not labor.*
- ▶ *Implied warranties require the product to reasonably do what it is intended to do.*

Refunds & Returns

There are no state laws that specifically regulate or require refund or return policies. However, Wisconsin businesses may choose to offer customers cash, store credit, or exchanges. Provided the goods are not misrepresented, each business may set its own refund/return policy including restocking fees.

Policies may differ for various items within the same store. For example, clearance or closeout items may be marked “sale final–no returns.” If you purchase an item that is defective, the store may require you to contact the manufacturer rather than replace the item or issue a refund.

Protecting Job Seekers

Many companies offer ways to “own your own business” by marketing and selling their products out of your home. Take great care when considering whether to become involved in business opportunities like these. Scammers make money from job scams and work-at-home schemes that target consumers looking to supplement their income. A job scam is when con artists charge upfront fees after making false promises to get you a job. A job scam that claims to allow remote work is a work-at-home scheme. Job seekers are affected by other scams as well.

Warning Signs for Job Scams

- Be suspicious of unsolicited job offers. Not all are illegitimate, but many are.
- Watch out for vague ads with no company name or address.
- Do not pay fees upfront. Most legitimate employment agencies will not charge you unless they actually succeed in getting you a job, and often the new employer will pay this fee.
- Get all promises in writing before you pay, including any return and refund policies and details on how you will be paid.
- Be aware of legal requirements, including any licenses, certifications, or restrictions on home-based business operations in your community.
- Be wary of promises to help you get a government job. No employment service can guarantee that you will qualify for a government job or arrange to get you special treatment.

Research Opportunities Carefully

- ▶ *Find out where the company is located and how long they have been in business.*
- ▶ *Check them out with the Bureau of Consumer Protection and the Better Business Bureau.*
- ▶ *Know what you will be selling, what’s similar on the market, and if the products you would be selling are competitively priced.*
- ▶ *Make sure your sponsor or recruiter can support claims about the product’s performance and the amount of money you can make.*

Direct Selling and Chain Distributor Schemes

Some companies require their new “business owners,” “partners,” or “affiliates” to purchase products upfront from a central distributor and resell those products directly to consumers at a markup in order to make a profit. This is known as single-level marketing. These companies often do not guarantee any wage, income, or return on investment to their salespeople.

When companies offer bonuses, new income streams, or continued employment to salespeople who enlist new salespeople, it is called multi-level marketing – sometimes known as pyramid selling or pyramid schemes.

In these cases, salespeople are often required to provide a cut of their earnings to the person who signed them up, who is required to provide a percentage of their earnings to the person above them, and so on; or to sell products purchased from the distributor ‘above’ them to the distributor ‘below’ them; or to practice other, similar company policies. This sales model can be lucrative for people near the top of the pyramid, but often leaves salespeople at the bottom without any income or even deep in debt.

These multi-level practices are known in Wisconsin law as chain distributor schemes, and are illegal. Companies engaged in this practice rarely describe themselves as multi-level marketing, preferring terms like “affiliate marketing” or “home-based business franchising.” Job seekers should be aware of this practice and avoid it.

Secret Shoppers

Fake promoters use online ads and emails to offer employment for highly paid secret shopper jobs with reputable companies. It’s a scam if they guarantee a job as a mystery shopper, charge a fee for access to mystery shopping opportunities, or ask you to deposit a check and then wire money somewhere else.



Protecting Travelers

Everybody needs a vacation once in a while, and nobody wants to spend that free time worrying about finances. Taking time off and traveling can be expensive, and scammers know that – and may try to rip you off.

Timeshares, Campgrounds, Vacation Clubs, and Recreational Property

Consumers should take their time and avoid being subjected to high pressure sales tactics often used in the sale of timeshares, campgrounds, vacation clubs, and recreational properties.

Protect yourself

- Get all promises in writing.
- Read the contract entirely before you sign.
- Find out if annual maintenance fees are required, how much they will be, and options for getting out of them in the future.
- Research the reputation of the seller, the developer, and the management company.
- Check for any limits on exchange opportunities, including plans offering “swap” arrangements with different resorts or campgrounds.
- Be wary of fraudulent companies offering to resell or exchange your recreational property or membership. Scammers often charge large fees upfront then cut off communication.
- Consumers have a five-day right to cancel timeshare contracts. Be sure you receive a copy of this in writing.
- Know what rights or protections are included in the purchase.
- American property laws generally do not apply to foreign timeshare contracts.

State Law Protects Consumers

- ▶ *People who sell timeshare and campground memberships must be licensed by the state. Contact the Wisconsin Department of Safety and Professional Services, (608) 266-2112 to inquire about an entity's licensing.*

Vacation Scams

Vacation scammers sell vacation certificates, which are nothing more than a form to request a vacation. Often, these offers are mailed out as postcards or flyers.

Many offers require making a purchase, obtaining a membership, or attending sales presentations before the certificate is issued or validated.

Research any vacation offer you consider

- Know if you are required to attend a sales presentation. If so, how many, how long are they, and for what purpose?
- If you are promised a prize for attending a presentation or sales pitch, they are required to give you the prize before the presentation begins.
- Get a breakdown of all additional costs and what is being included at no cost.
- Note that travel, lodging, or other vacation offerings may not allow use on holidays, weekends, or during prime tourism seasons.
- Know what taxes, transportation, meals, or other fees are required.
- Get cancellation, refund, and rescheduling policies in writing. Offers may be non-refundable.



Small Claims Court

Any individual or corporation doing business in Wisconsin can sue or be sued in small claims court. *Wis. Stat. ch. 799* governs small claims actions. Small claims court is intended for settling disputes of \$10,000 or less without the use of an attorney, but you still have the right to hire an attorney for small claims actions.

A guide to small claims

The small claims court clerk at any county courthouse can supply you with the necessary forms (a summons and a complaint form) to begin your action. The clerk can also tell you where to file the completed forms.

- Copies of the filed forms must be “served on” or delivered to the defendant.
- After your claim is filed, the court will typically set an initial informal conference to review the facts in your case. Many small claims court cases are settled at these informal conferences, so come prepared to argue your case.
- If you are not satisfied with what is done at the informal conference or by a court commissioner, you maintain the right to have your case heard by a circuit court judge in a full trial.
- If you win the case, you can ask the court to include court costs and any money you spent as part of the settlement.
- Keep in mind that it will be your responsibility to collect the judgment settlement from the defendant. The court will not do this for you.



Additional Resources

Information about all these topics and more can be found at the Department of Agriculture, Trade and Consumer Protection's website at datcp.wi.gov.

The Bureau of Consumer Protection's webpage can be found at that site or by going to ConsumerProtection.wi.gov.

Fact sheets about specific consumer protection issues can be found at ConsumerFacts.wi.gov.

A digital version of DATCP's Landlord-Tenant Guide outlining laws regarding rental housing can be found at LandlordTenant.wi.gov.

View DATCP's [Ready Reference Guide](#) on our website for a directory of additional resources available to you regarding a variety of consumer topics.



Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison, WI 53708-8911
datcp.wi.gov

Contact Information:

Call our toll-free hotline at (800) 422-7128 or
email us at DATCPHotline@wisconsin.gov.

To file a complaint visit our website:

ConsumerProtection.wi.gov.