

# Consumer Protections

Last updated on February 13, 2025.

Phone and Internet

## Wisconsin Do Not Call Registry

If you are receiving unwanted telemarketing calls and/or text messages, you can add your number to the Wisconsin Do Not Call Registry. This is a free service which will make sure you receive less telemarketing calls and/or text messages.

**NOTE:** This service does not stop these calls, it helps reduce the amount of calls you receive.

Common people that scammers try to impersonate over the phone:

- Social Security Administration (note: the social security administration will not call you directly. They primarily use mail for communication.)
- IRS or US Treasury
- Utility shut-off
- Law enforcement
- Friend and Family Scam

General Rules to protect yourself from phone scammers:

- Avoid paying for things over the phone or sending money by gift card or money transfer (Western Union, MoneyGram, Venmo, Zelle or prepaid card). If you must do it over the phone, ensure that you verify their authenticity.
- NEVER give out personal or sensitive information to someone you do not know.
- Never pay for anything that is said to be a “free prize”
- If you feel like the person on the phone is rushing you, it is likely a scam.

**Online security:**

- Shop only from familiar companies. If you are unsure if a website or company is legitimate, it is important to do your research. Many times a quick google search can confirm if a site is in fact a scam.
- Use virus protection, spyware protection, or firewalls.
- Use strong passwords and change them often.
- Delete messages from people you don't know. Do not open them.

Common online impersonation scams online:

- Bank notice scams
- Shipping notice such as UPS or Amazon scams
- Renewal notice scams
- Pet scams
- **Pig Butchering Scams** (Long-term online scams) - some of the most legitimate looking scams out there.
  - This scam is one of the hardest to catch because many times you can talk to a real person and verify their identity and still be caught in a scam. Here are a couple of ways to spot one of these types of scams:
    - Receiving texts from a “wrong number”
      - If you do not recognize the number that is texting or calling you, do not respond. They may even call you the wrong name or send a picture of something you did not order. Do not respond. Delete the texts.
    - A stranger you met online starts talking to you about crypto.
      - Do not trust a person online who is guiding you through investing in crypto. Talk to a financial advisor in person.
    - Someone on a dating app starts “love bombing” you, they overshare intimate details about their lives, or are constantly available online.
      - If you cannot meet them in person, it is most likely a scam.
    - Using emotional manipulation tactics to get you to pay them money.

→ These scammers may work to gain your trust and then use that relationship against you. They may tell you that they need you to invest in crypto to help their sick child or dying parent.

- A friend or family member asks you to invest in crypto.

→ This can be the most insidious way a scammer can get to you. These scammers play the long game, so while your friend or family member might not know it is a scam yet, they may be able to convince you to also invest in the scam. Many times this happens because the scammer can make it look like you are making money that isn't there or "guarantee returns" which do not exist.

- Someone asks you to download a special crypto app or exchange software.

→ Note that this can look very legitimate. Some may even run their scam through an actual crypto app, so it is easy to be convinced of the scam's legitimacy.

- You are told that the account will be under your name but they will guide you on how to invest.

- You are asked to pay a huge tax bill to collect your investment earnings.

→ This is a huge red flag. Do not pay anything to collect your investment earnings.

**Note:** Check out Wisconsin Department of Financial Institution's (DFI) [Investor Education page](#), which includes a guide to help you avoid financial fraud and will soon include a scam tracker database collecting reports of confirmed scams.

### **Phone/Tablet Application Security:**

Many apps have "in-app purchasing" which allows you to pay for different features on an application without leaving the app. While this is convenient in many ways, it

can also lead to some security issues. The following are common issues:

- Children charge money to their parents' accounts without realizing it.
- You may spend a lot of money without realizing it. Many times the in-app purchases are subscriptions and charge you every month.
- Unencrypted data isn't secure. It is important to be aware that some apps collect data like your name, email address, phone number and leave it unencrypted or unsecure. This can make it easy for scammers to steal your information.
- Location data may be shared or sold without your knowledge. Many apps require your location to work, such as weather and GPS apps. However, there are some apps that only request your location information to sell the information to advertisers. It is best practice to turn off sharing your location with your apps unless it is absolutely necessary.

Home

### **Home Improvement:**

If you hire a contractor to work on your home, you want to keep the following things in mind:

- If possible, hire a local contractor, especially if your area was recently hit by a storm or natural disaster.
- Get more than one cost estimate in writing before deciding on a contractor.
- Ask the contractor for references and reach out to them to get their opinion of the contractor's work.
- Make sure to ask the contractor whether they will be using a subcontractor to perform part of the job. If so, find out who the subcontractor will be and try to get references for their work as well.
- Make sure you get all details about the project in writing including, estimates, contracts, warranty information, start and end date, what work is to be completed, and what materials will be needed.
- If you have a cancellation period, get multiple copies of the cancellation forms from the contractor.
- Be careful if a contractor promises to pay or rebate portions of an insurance deductible.

- Request lien waivers from anyone you pay for home repairs (these are like formal receipts).
- **Never pay with cash or checks made out to cash.** You want to make sure you have a receipt of the payment.
- It is also a good idea to check with the Bureau of Consumer Protection and the Better Business Bureau to see if any complaints have been filed against the contractor or subcontractor.

\*Also beware of **transient crews** who show up after major storms or in summer months offering construction or repair work. Before signing a contract, look them up online or in the phone book. Contact your municipal clerk to see if the crew has been approved to work in the area.

- If they begin to work on your property without your consent or do not leave when asked, call the police.

### **Door to Door Sales**

These salespeople can only sell from 9:00 a.m. to 9:00 p.m, unless they are a door-to-door nonprofit group. In most cases, the Wisconsin Consumer Act gives you a three-day right to cancel a sale that began with a door-to-door solicitation. Wis. Stat. chapter 423, subchapter II.

### **Junk Mail**

Junk mail may seem harmless, but it is sometimes used by scammers to commit fraud or identity theft. You can reduce the amount of junk mail you receive by removing your name from large mailing lists sold to direct mail marketers by registering with DMAchoice at [DMAchoice.org](http://DMAchoice.org) or by calling (212) 768-7227 ext. 1888. Additionally, you can opt out of unwanted credit card offers at [OptOutPrescreen.com](http://OptOutPrescreen.com) or by calling (888) 657-8688 and selecting opt-out.

### **Purchases**

#### **Refunds and Returns:**

Although there are no state laws that regulate or require refund or return policies, businesses may choose to offer customers cash, store credit, or exchanges. Policies may differ based on the item and the store.

### **Job Seekers**

- Be cautious when working with companies that offer to help you “own your own business”.
- Get all contracts or promises in writing.
- Beware of ads with no company name or address.
- Do not pay any upfront fees. You should not be required to pay anything until you actually secure a job and then typically your new employer will pay the fee.

### [Protection Money, Debt & Consumer Issues](#) [Consumer Protection & Complaints](#)

How helpful do you find the information on this page?

- ☐ Not helpful
- ☐ Somewhat helpful
- ☐ Very helpful

Save

Please tell us why this page wasn't helpful

- ☐ N/A
- ☐ Not related to my issue
- ☐ Not enough information
- ☐ Unclear information

Comment

### [About text formats](#)

#### **Plain text**

- No HTML tags allowed.
- Lines and paragraphs break automatically.
- Web page addresses and email addresses turn into links automatically.

Save

Print

[Table of Contents](#)

## Our Partners

This website is supported by

**LSC** | America's Partner  
for Equal Justice

LEGAL SERVICES CORPORATION

LSC's support for this website is  
limited to those activities that are  
consistent with LSC restrictions.

**WisTAF**  
investing in justice for all

---

PDF downloaded from <https://www.wislawhelp.org/page/108/consumer-protections>