THE WISCONSIN

Senior Guide

Wisconsin Department of Agriculture, Trade and Consumer Protection

Consumer Protection for Wisconsin Senior Citizens

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 providing services to inform, educate, and protect the public – especially our seniors.

This booklet is a summary of common consumer protection issues facing Wisconsin's senior citizens.

Additional details and more consumer protection topics are available on our website or upon request. Please contact us at the Bureau of Consumer Protection for additional information or further assistance.

For other matters, the Bureau of Consumer Protection will gladly assist by identifying the most appropriate state agency or organization to contact.

Copies of this booklet and other consumer protection educational materials are available from:

Department of Agriculture, Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911
datcp.wi.gov
DATCPHotline@wi.gov
1-800-422-7128

Contents

Avoid Scams

Beware of imposters. Legitimate businesses or government agencies will not ask for your personal information or threaten you. The best defense against imposter scams is to not respond.

Don't wire transfer money or pay by gift card. Money sent via wire transfer or money cards is practically impossible to track. Ignore requests to pay by gift cards or prepaid cards. Gift cards are for giving, not for making payments. Pay by credit card (not debit card) whenever possible, since you can dispute charges easily.

Just don't answer. Be cautious when responding to telemarketers, door-to-door sellers, email, and text messages. Instead of responding to unsolicited offers, decide when and where you want to go shopping.

It's personal – keep it that way. Never give out your Social Security, credit card, or bank account numbers or other personal information to anyone you don't know who contacts you.

You don't have to pay if you are a winner. Anyone who demands an upfront fee or purchase for a prize is trying to scam you.

Protect your computer. Don't click on links within unsolicited emails. Don't enter personal information on unfamiliar websites. Make sure that you have updated antivirus software installed, use a firewall at all times, and use strong passwords you change regularly.

Do your research. Do business with companies you know or that come recommended by those you trust. Get as much information as you can about a business or charity before you pay. Check out a business with the Bureau of Consumer Protection before you act.

Before you act, **Stop, Think, Ask** and get it in Writing.

If it sounds too good to be true, it probably is a scam!

Protect Yourself

Monitor your bills/statements. Review your bank statements and bills for unauthorized charges as soon as they arrive. Report any issues as soon as possible. If your bill or statement does not come at the normal time, call and ask about it.

Put a security freeze on your credit reports. It is free and allows you to prevent an extension of credit, such as a loan or a new credit card, from being approved without consent.

Check your credit report regularly. You can obtain one free credit report per year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion). To access your free credit reports, visit annualcreditreport.com or call 1-877-322-8228.

Wisconsin Law for Seniors and the Disabled

Wisconsin law (Wis. Stat. § 100.264) provides additional punishment for those who prey upon or take advantage of senior citizens or the disabled.

The law permits courts to impose additional forfeitures of up to $10,000 for violations of consumer laws and rules including:

- False advertising
- Mail order
- Home improvement
- Vacation offers
- Deceptive employment offers
- Landlord/tenant
- Telecommunications
- Motor vehicle repair

The law may be applied in a number of situations, including the guilty person knowing that the victim was a senior (age 62 and older) or disabled. The court must require that restitution be paid before any additional forfeiture.

Protect Your Personal Identity

Identity thieves can use any combination of your name, Social Security number, mother's maiden name, ATM pin, date of birth, or bank account numbers to steal money from you and commit financial fraud or identity theft. Keep your private information private.

Obtain your credit report FREE from each of the three major credit reporting agencies each year.

Identity Theft Tips

- Do not carry your Social Security number.
- Limit the number of identification cards and credit cards you carry and know which ones you have with you.
- Shred bills, receipts, credit card offers, and other items that contain personal or financial information.
- Stop pre-approved credit card offers to help prevent identity theft or fraud. Call 1-888-567-8688 or visit optoutprescreen.com.
- Review your credit card and financial statements when they arrive and report suspicious activity to your card provider as soon as possible.
- Never give out personal information over the phone or online unless you initiate the contact.
- Make certain you have firewall, antivirus, and anti-spyware protection on your computer, and use strong passwords.

- Check your credit report regularly. Obtain your credit report FREE from each of the three major credit reporting agencies each year by calling 1-877-322-8228 or at annualcreditreport.com.
- Keep personal information and sensitive documents locked up.
- Register for the Wisconsin Do Not Call Registry at NoCall.Wisconsin.gov or 1-888-382-1222. You must call from the telephone number you wish to register.

Recover Your Personal Identity

Many identity theft cases go for a long time before the victim finds out that they are being robbed. If you feel that you have become a victim of identity theft or fraud:

- Contact your financial institution and your credit card provider.
- Report it to local law enforcement.
- Notify the three major credit reporting agencies.
- Request that an "alert" or a "freeze" be placed on your credit report.
- Contact the Wisconsin Bureau of Consumer Protection.

The recovery process will be much easier to work through if you keep an inventory list of all credit card and bank account numbers, expiration dates, and phone numbers available for contacting the institutions that issued each card.

Junk Mail

Thieves 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.

Fraudulent credit card offers can target people who are having credit problems and have not been able to get credit elsewhere. Scammers can also use unsolicited pre-approved credit card offers to trick consumers into giving up sensitive information. The scammer uses this information to steal the victim's identity and commit additional fraud.

Tips

- Reduce as much junk mail as possible from reaching you.
- If you receive mailed offers in someone else's name, return them to the sender.
- If the mailed offer is addressed to you and you do not want it, shred it.

Reduce junk mail

- **Mailing lists** – you can eliminate your name from the large mailing lists sold to direct mail marketers by registering with DMAchoice at DMAchoice.org or by writing to:

  DMAchoice
  Direct Marketing Association
  PO Box 643
  Carmel, NY 10512

- **Credit card offers** – you have the right to opt out of unsolicited credit card offers by visiting the Opt-Out website at optoutprescreen.com or by calling 1-888-567-8688. Make sure to select "Opt-Out," not "Opt-In."
- **Direct mailings** – to reduce other types of mail, write directly to the companies that are sending you the junk mail and tell them to stop.
- **Sexually oriented** – to stop this type of mail, fill out the proper paperwork at your local post office.

Reduce unwanted email

- The Email Preference Service (eMPS) is a consumer service sponsored by the Direct Marketing Association (DMA). To reduce email, you may register free every six years at ims-dm.com/cgi/optoutemps.php.

Cramming

Cramming is when companies add charges to your telephone or credit card bill for services or products such as voice mail, web design, internet access, or club memberships that you never authorized.

Many times cramming charges occur after you fill out a contest entry form, product coupon, or other promotional materials. These documents may have very fine print that includes an agreement to buy a service that will be charged to your phone number or credit card bill.

Other times, cramming may occur when you agree to switch your phone carrier.

Tips

- Cramming charges can be minimal and easy to overlook.
- Review your bills closely every month and dispute charges for services you did not request.
- 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 return voice mail or text messages to numbers that you do not recognize. A crammer may see the number you are dialing from and process an unauthorized request fee service.
- Be cautious of websites that ask for your phone number. There have been cases where consumers entered a phone number to get a "free offer" and wound up with other services or club memberships charged to their phone bill.

Wisconsin Do Not Call

Getting your landline and cell phone numbers on the Wisconsin Do Not Call Registry is free and available to residential phone customers in Wisconsin. Sign up for the Do Not Call Registry at NoCall.Wisconsin.gov or by calling 1-888-382-1222. You must call from the telephone number you wish to register.

The Wisconsin Do Not Call program is helpful for reducing (not stopping) unsolicited telemarketing calls and text messages. While the program does not stop all illegal telemarketing calls, the program does help government agencies crack down on illegal practices from within the United States and Canada.

Exemptions include calls (Wis. Adm. Code s. ATCP 127.10)

- To current customers.
- From non-profit organizations seeking donations.
- Made for polls, surveys, and political purposes.

Tips

- If the caller asks for payment using money transfers (i.e., MoneyGram, Western Union) or asks for the PIN number from a gift card or prepaid card (i.e., iTunes , GooglePlay, MoneyPak, or Reloadit packs) – HANG UP!
- Beware of callers who ask you to send money or buy something sight unseen over the telephone.
- Never give out your credit card, Social Security, 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 be rushed into anything.
- If a caller offers to send a messenger to your home to pick up your payment – HANG UP!

- Beware of "spoofing." Crooks can make any name and number appear on your caller ID – such as your bank, a neighbor, or even your own phone number.

Imposter Scams

An imposter is someone pretending to be someone else. You may receive a call or email claiming to be from a government agency or a familiar business. They tell you that you owe money immediately or you could be arrested or sued. They may threaten you and ask you to wire the money or pay using a prepaid debit card.

Common Imposter Scams

- Social Security Administration (SSA). Threatening calls about supposed problems with your Social Security number. The SSA will not contact you, out of the blue, asking you to verify your Social Security number or tell you to wire money or put money on a gift card.
- IRS or US Treasury. Threatening calls that you must pay now for tax violations or be arrested, sued, or deported. The IRS will not contact you by phone. They will not make threats.
- Computer Problems and Screen Pop-Ups. The caller claims to be from a well-known company like "Microsoft" or "Google." They say they have detected a problem with your computer and can fix it for you. These callers want you to pay for their "services" on the spot so they can obtain your credit card information. Then they access your computer remotely so they can steal personal information and download damaging software known as "malware" that will allow them to continue to access and even control your computer.
- Utility shut off. The caller states you have not paid your utility bill and someone is on the way to disconnect your service unless you pay immediately on the phone.

- Law enforcement. The caller states that there is an outstanding warrant for your arrest or you have failed to appear for jury duty. The caller asks you to pay immediately to avoid prosecution or jail time.

What to do

- Do not trust caller ID. The information could be "spoofed," meaning the phone number is misrepresented.
- The government does not make unsolicited calls.
- If you receive a call or email that you are not expecting, CHECK IT OUT! Only call back directly using information from a bill to verify what you were told.
- Never give a caller access to your computer.
- Never pay by wire transfer or by pre-paid debit or gift cards. Hang up on the call or delete the email.
- Report it to the Bureau of Consumer Protection at 1-800-422-7128. Your reports help protect others.

Robocalls

Robocalls are those annoying and often relentless automated calls that deliver pre-recorded messages.

Robocalls may include a message that claims to be offering a lower credit card or mortgage interest rate or information about home security systems, Medicare benefits,"free" medical equipment, or fraudulent health care discount plans.

Hang up on unwanted robocalls.

What to do

- Do not answer unrecognized calls and do not rely on caller ID as it could be misrepresented, or "spoofed."
- Hang up on unwanted robocalls.
- Never press any buttons to respond to the call, even if the message says that doing so will remove you from their list.
- Never try to talk to a live operator, because that will increase the number of calls to your phone.

Grandparent Scams

A caller pretends to be your grandchild and begs you to send money immediately. They also beg that you keep the call a secret from other relatives, especially the grandchild's parents. The money may be to get out of jail, pay for a car repair, get home from a foreign country, or pay for an emergency room or hospital visit. Sometimes a third person becomes involved, pretending to be a police officer, doctor, lawyer, or bondsman to confirm the bogus story.

This is a scam that many grandparents get caught in every year. Why? Because the scammers are very convincing and very slick at pulling it off! Thieves are even using email to pull off this scam, and it is working.

DO NOT wire any money to the scammers!

What to do

- Ask personal questions to verify the caller's identity using questions only a close family member would know.
- Do not fill in the blanks for the caller. If the caller says, "It's your granddaughter," respond with "Which one?"
- Contact your grandchild using a number you know. If he or she cannot be reached, contact another family member to verify the grandchild's whereabouts.
- If you cannot reach a family member, contact the non-emergency number of your local police or the Bureau of Consumer Protection.
- NEVER wire money to scammers! You will not get it back.

Phishing

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

Legitimate companies never contact you and ask for account information over the phone.

A con artist may pose as a representative from your financial institution or another familiar business and ask to verify your account numbers. Just remember that legitimate companies should never contact you and ask for account information over the phone because they already have it on file.

Phishing may also take the form of fake shipping emails made to look like they are from a legitimate shipper like UPS or FedEx. The emails claim that you have a package waiting or that there is a problem with a delivery. The recipient is prompted to open an attachment for the shipping details or to click a link to review their "account."

Tips

- DO NOT RESPOND if you receive an email or text message alerting you to a possible problem that requires you to update, validate, or confirm your account information with a business. Instead, contact the company directly using their legitimate number from your paperwork or local phone book – not the number provided by the scammer.
- Do not click links in unsolicited emails.

- Do not open attachments until you have contacted the sender first to verify the contents and security of the attachment.
- Do not click on pop-ups that appear as internet ads on your computer.
- Change your browser's settings to block pop-ups.
- Grammatical errors are a red flag that the email is not from a professional, reputable, and legitimate business.
- Spot the scam. If you hover your mouse over a link in an email (do NOT click your mouse!), the URL that the link directs you to will typically appear in the bottom of your browser window.

Spoofing

With spoofing, scammers block their real identities from showing up on your caller ID, email, or text messages. The scammer will appear to be a friend, official site, or trusted source that you feel comfortable responding to.

If you open or respond to a message or link that is intentionally infected with a virus, not only can the virus destroy your computer files, it can grab the addresses of your friends and send them a virus as well. The scammer's message to your friends will appear as a trusted message coming from you. When they open or respond to your supposed message, the cycle continues with their friends.

Tips

- Use antivirus and anti-spyware protection, firewalls, or other filtering software and keep it updated.
- Use strong passwords and keep them updated.
- Delete messages from unsecured sources without opening or responding to the messages.

Romance Scams

Social media, dating websites/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 photo they have found online. They use this to gain trust and love from a victim in order to get them to send money for travel expenses, legal help, medical bills, or any number of other issues.

If you are communicating with someone using an online dating tool, ask questions, look for inconsistent answers, and take it slowly. Also, check the person's photo using the "search by image" feature in your search engine – if the same picture shows up with a different name, that is a warning sign.

Tips

It is possible you are being targeted for a romance scam if your online love interest:

- Claims to be from the United States but is currently "traveling," "deployed with the military," or "working overseas."
- Professes love for you almost instantly.
- Asks you to leave the dating site and communicate by email or instant messages.
- Requests that you send personal information including Social Security, bank account, or credit card numbers.
- Asks you to cash checks for him/her.
- Makes excuses for not meeting in person, such as last-minute financial, medical, or family emergencies.
- Asks you to send money by wire transfer.

Charitable Solicitations

Organizations sometimes pay telemarketers to conduct professional fundraising for them, and in some cases the telemarketers keep a large percentage of the donations.

Only donate to organizations that you know and trust.

Be very cautious of

- Any organization that pressures you to donate on the spot.
- Groups sending you free gifts in order to get you to donate.
- Charities or organizations that do not disclose how much of the money collected is used for charity and how much goes for salaries and administration.
- Sound-alikes and look-alikes whose names, logos, and websites are very similar to those of legitimate, well-known charities.
- Charities or organizations that use excessively tearful or emotional appeals.
- Thank you letters that include an appeal for additional money.
- Fraudulent fundraising that pops up after natural disasters or other tragedies strike.

Before you donate

- 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: 1-608-267-1711 or check online at wdfi.org.
- Check out a charity through the Better Business Bureau at wisconsin.bbb.org/charity.

Gift Cards

Gift cards work like a gift certificate, but resemble a credit card and are identified by a specific number or code rather than an individual's name. Losing a gift card is the same as losing cash.

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

How are consumers protected?

- **Expiration dates** – must be clearly disclosed and be at least five years from date of purchase on most cards, but cards given as a reward or promotion for making a purchase can expire in one year.
- **Expiration date extensions** – must be given on cards which allow for the addition of more money after their initial purchase. The card may not expire for at least five years from the last date additional money was added.
- **Dormancy, inactivity, and service fees** – are allowed when a card has not been used for more than one year.

Prepaid cards not covered by Federal Reserve rules:

- Calling cards and loyalty or promotional cards.
- Reloadable cards not marketed as "gift cards."
- Paper gift certificates issued for tickets, admission, spa services, and coupons.

Warranties

There is no difference between the terms "warranty" and "guarantee," but there can be a big difference between the warranties of two similar products manufactured by different firms.

The Magnuson-Moss Warranty Act (15 U.S.C §§ 2301-2312) does not require manufacturers to issue warranties on their products, but if they do, the warranty must be easy to read and understand. Every term and condition must be spelled out in writing.

Before making a purchase, know whether the product or service is covered by any warranties. A ***FULL*** warranty typically covers defective products that are fixed (or replaced) 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 or your money back.

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 a restocking fee requirement.

Policies may differ for various items within the same store. For example, clearance or closeout items may be marked "final sale–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.

Suggested questions to ask

- Is there a time limit for returns?
- Will I be able to get a cash refund?
- Do I have to use store credit within a specified time period?
- Will the store accept returns of sale merchandise or seconds?

Tip

Before you sign a contract or agree to a special-order item, ask the business about refund and return policies. Insist that delivery dates be written into your contract and make sure you can get your money back if the shipment is late.

Rebates

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

Manufacturers may

- Offer a specific cash refund, coupon, free product, or service.
- Set specific expiration dates, proof-of-purchase requirements, per-household limits, and other restrictions.

Tips

- Follow the rebate requirements carefully.
- Consider the true value of the rebate being offered, especially if you are being offered in-store credit on future purchases rather than money back or actual money off of the purchase.
- Keep copies of rebate forms and a record of the date that you mailed the rebate in.

Mail Order

The Wisconsin mail order law (Wis. Stat. s. 100.174) covers any personal order where the seller solicits and accepts payment without face-to-face contact.

Under the law, the seller must ship prepaid merchandise or make a full refund within the delivery time shown on the original order form or ad, 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 this happens, you may:

- Contact the seller and cancel the order. They must then promptly send you a refund.
- Contact the seller within 30 days agreeing to a delayed delivery date.
- Do nothing. The seller must then ship or refund payment within the extended delivery time stated, but not exceed 30 days after the original delivery period.

Unsolicited Merchandise

Under Wisconsin law (Wis. Stat. s. 241.28), unsolicited merchandise is considered a gift and may be kept without any obligation to the sender. Do not be pressured by companies that make a practice of mailing unordered merchandise on a "trial basis," then send phony invoices.

Negative Options

A negative option is a marketing plan that basically states: "We will keep sending you our product or providing you with our service until you tell us to stop." With a negative option plan, it is the responsibility of the consumer, not the seller, to cancel a contract or order.

Unless you say "NO" within the specified time period, you will be charged for the merchandise and shipping. To protect yourself, contact the company in writing to cancel any future orders and return all unwanted goods. Otherwise, your account may be turned over to a collection agency.

Advance Fee Loan Scams

Beware of ads promising guaranteed loans, debt consolidation, credit repair, or similar claims. Be even more cautious if the offers claim that they can help those with the worst of credit problems. In many cases, you will be asked to send money in advance, but will receive little or nothing in return.

Contests, Lotteries, Sweepstakes, & Prize Promotions

Whether it is a bogus contest, lottery, sweepstakes, or prize promotion, scammers will send an authentic looking check, cashier's check, or money order to be deposited into your bank account.

How the scam works

The con artist requests that you send back a portion of the money for shipping, taxes, processing fees, or other reasons. These checks are fake but look very real. Even bank tellers may be fooled. It may take weeks for the forgery to be discovered and the check to bounce. By that time, the con artist has your cash, and you will owe your bank for any money withdrawn and any bounced check fees.

Tips

- Never agree to pay to claim a prize or a gift.
- If they request that you wire them money, it is a scam and you will not get your money back! End the transaction immediately.
- Do not enter foreign lotteries.
- Resist any pressure to "act now."

If they request that you wire them money, it is a scam!

Common scams

International Lotteries
In the United States (per 18 U.S. Code § 1953), it is illegal to use the mail or telephone to play lotteries across national borders or state lines. By responding back to the scammer to enter or play the lottery, you are breaking the law.

Phony Sweepstakes
Scammers will try to get you to send money or buy something in order to redeem the prize.

Magazine Sweepstakes
Magazine sellers offer sweepstakes as a way to attract new customers. You don't have to make a purchase to enter the sweepstakes and you will have the same chance of winning.

Check Overpayment Scam
Scammers will intentionally overpay for items you have posted for sale. They act like it was an honest mistake and will request that you return the overpayment portion. By the time their check bounces, the scammer will have the money and the purchased item in hand.

Although you can withdraw the deposited money quickly, it may take weeks for the forgery to be discovered and the check to bounce. You will then be responsible for paying back any money withdrawn and any overdraft fees.

Fake Check Scams
There are many variations of the fake check scam, but scammers often claim to be in another country and say that it is too difficult or complicated to send you the money directly from their country, so they will arrange for someone in the United States to send you a check.

Inheritance Scams

Scammers are incredibly slick at convincing seniors that they have inherited a large sum of money from a long-lost relative who died overseas. The scammer will pose as an attorney or bank official, asking you to call him with your bank information so he can make arrangements to get the money to you. **Do not fall for it!**

In some cases the scammer will send you part of the supposed funds and ask you to pay him for the taxes and processing fees. You will be told to act immediately and keep the transaction secret.

The details vary. Sometimes the scammer claims to be a government official who needs help transferring millions of dollars from his country to a bank in the United States. Or they pose as a rich person on their deathbed, looking for someone to help distribute their wealth to worthwhile charities. Some con artists will go to great lengths to make everything sound plausible; others rely on your wishful thinking to fill the gaps in the story.

Bottom line – it is a scam! You will never get back any money you wire to the scammer.

Business Opportunities

When considering whether to become involved in a business opportunity, use our suggestions to help guide your decision making process.

Tips for all business opportunities

- 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 similar products/services are already on the market, and whether the product/service is competitively priced.
- Make sure your sponsor or the person recruiting you can support claims about the product's performance and the amount of money you can make.

Work-At-Home Schemes

Scammers make money off of work-at-home schemes by requiring purchases of training manuals, craft kits, or potential customer contact information.

Scammers target seniors looking to supplement their income. They will take your money, then reject your finished projects as being inferior, or send you worthless contact information.

Tips

- Watch out for vague ads with no company name or address.
- Get all promises in writing before you pay, and know the return and refund policies.

- Get written details on how you will be paid for your efforts or services.
- Do not give out your Social Security number or other personal information.
- Find out if there is really a market for your work.
- Be aware of legal requirements, including licenses, certifications, or restrictions on home-based business operations in your community.

Job Scams

A job scam is when con artists charge upfront fees after making bogus promises to get you a job. Or they will send you advice on writing resumes or lists of companies that they have gotten for free from public directories.

Money-back guarantees will not be worth the paper they are written on. Fraudulent employment services will use an endless string of excuses for why you are not entitled to a refund.

Tips

- Do not pay upfront fees. Most legitimate employment agencies do not charge unless they actually succeed in getting you a job, and often it is the new employer who pays.
- Be especially cautious of requests to wire payments. Recovering wired funds is nearly impossible.
- Know what services are being offered.
- Get all promises in writing, including money-back guarantees.
- 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.

Secret Shoppers

Fraudulent promoters use newspaper ads and emails to create the impression that they are a gateway to lucrative mystery shopper jobs with reputable companies.

The scammers will even promote a website where consumers can supposedly "register" to become certified mystery shoppers with them. Be cautious of promoters who:

- Require mystery shoppers to be certified.
- Guarantee a job as a mystery shopper.
- Charge a fee for access to mystery shopping opportunities.
- Ask you to deposit a check and then wire some or all of the money to another person or business.

Investment Seminar Scams

Investment scams are often promoted at seminars held in hotel or resort conference rooms. Seminar salespeople use high-pressure sales tactics to push you to act on the spot.

Be wary of promotional materials, sales pitches, or offers that make these claims:

- You can earn big money fast, regardless of your level of experience or training.
- The program or business opportunity is offered for a limited time.
- The deal is a "sure thing" that will deliver financial security for years to come.
- You will reap financial rewards by working part time or at home.
- You will be coached each step of the way to success.

- The program worked for other participants – even the organizers.

Seminar tips

- Take your time and do not be rushed into buying on the spot.
- Investigate the business you are considering investing in.
- Be wary of "success stories" or testimonials of extraordinary success. The claims could be coming from someone who was paid to make such glowing statements.
- Be cautious of seminar representatives who are reluctant to answer questions or who give evasive answers to your questions.
- Get investment qualification requirements and the company's refund policy in writing.

Financial Investing

Be on guard against financial investment scams and fraudulent financial advisors, especially those that target seniors.

Report discrepancies or anything suspicious such as a missing payment or an unauthorized withdrawal.

Tips before investing

- Only deal with businesses, advisors, and other organizations you already know or that have been recommended.
- Contact the Wisconsin Department of Financial Institutions and the Bureau of Consumer Protection to find out if the company has any complaints filed against them.
- Check out the company with the Better Business Bureau.

- Look up the company in your area and for the area the company is located.
- Search the internet using the company name and the word "complaint" or "scam" to see if complaints have been filed.
- Get all key details of a significant offer in writing.
- Be cautious if the people making the sales pitch only focus on the benefits or the promised returns and rush over the costs and potential risks.

Tips after investing

- Closely monitor credit card bills and bank statements. Report any discrepancies or anything suspicious such as a missing payment or an unauthorized withdrawal.
- Watch for cash shortage when you should have enough money coming in.
- Monitor for signs of identity theft or financial fraud by your financial advisor. Get your free credit report online at annualcreditreport.com or by calling 1-877-322-8228.

Timeshares, Campgrounds, Vacation Clubs, and Recreational Property

Before you purchase any of the above

- Take your time and avoid being subjected to high pressure sales tactics often used by sales people.
- Get all promises in writing and insist on reading the contract carefully 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, developer, and the management company.

- Check for any limits on exchange opportunities, including plans offering "swap" arrangements with different resorts or campgrounds.
- If a point system is used, get written details of what the points cover and how they work.
- Ask and understand if you have a right to cancel the timeshare contract. Get copies of this in writing.

Before you resell

Be wary of fraudulent companies offering to resell or exchange your recreational property or membership. Scammers often charge large listing fees upfront with promises that never materialize.

Default Protection

Know what rights or protections are included in the purchase. Find out if the builder or management company has financial problems or defaults. Also, check to see if your contract includes clauses concerning "non-disturbance" and "non-performance."

Check to see if the seller of the timeshare and campground memberships is licensed. Contact the Wisconsin Department of Safety and Professional Services: 1-877-617-1565.

Vacation Offers

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

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

Tips

- 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, Wisconsin Prize Notice law (Wis. Stat. s. 100.171) requires that you receive the prize before the presentation begins.
- Get a breakdown of all additional out-of-pocket costs or verification of items or services being included at no additional fees, charges, or costs.
- Get all restrictions in writing – travel, lodging, or other vacation offerings may be prohibited on holidays, weekends, prime tourist periods.
- Know what taxes, transportation, meals, or other handling fees are required.
- Get cancellation, refund, and rescheduling policies in writing. Promoters often keep all or part of the money under nonrefundable policies.
- Compare the vacation offer to what a travel agent can provide or what you can get by doing your own planning.

Telecommunications

Cable, 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 that you cannot easily cancel.

In most cases, providers are required by Wisconsin law (Wis. Adm. Code ch. ATCP 123) to furnish you with a copy of any contract terms and conditions and limitations for your services, including:

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

Purchasing tips

- Find out what phone, internet, and video service options are available in the area you intend to use the services.
- Check for discounts available to new subscribers or for purchasing a package of bundled services. Get all details of the offer in writing.
- Get written details about early termination fees for disconnection of service – especially if you were to drop one component of a bundled service.
- Immediately after you buy your phone, test it in the places where you intend to use it. If it does not perform as advertised, take it back.

Get written details about any early termination fees for disconnection of service.

Senior Living / Housing

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

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

Tips 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 return of your original investment is dependent upon the sale of your unit (or not), 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 or your estate.
- Get written details on how the funds will be secured to ensure payment of a future buy back.

Door-to-Door Sales

Consumers often complain about door-to-door sales of home security systems, hearing aids, magazines, and window replacements or other home improvement projects.

Under Wisconsin's Direct Marketing law (Wis. Adm. Code ch. ATCP 127), before door-to-door sellers say anything beyond a short greeting, they are required to state their name, company name, and type of product/service they sell.

Traveling sales crews working in Wisconsin

- May be required under the local municipality to have a registration stamp placed on the certificate of registration prior to selling door-to-door in that community.
- Can only engage in sales activities from 9:00 a.m. to 9:00 p.m.
- Cannot claim to be engaged in a contest to win cash, scholarships, or some other prize.

Tips

- Get all promises and details of agreement offers in writing.
- Get two copies of the cancellation forms from the seller.
- When purchasing service plans for hearing aids, avoid duplicating coverage with your existing plans.
- When health care tests are involved in the possible sale, ensure that the tester is licensed or certified.
- Request a free trial period to evaluate the product/service.

Home Improvement

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

Tips

- Try to hire a local contractor to do the repairs, especially if the area was recently hit by a storm or natural disaster.
- Know whether the contractor will be subcontracting your job, and if so, who will actually be doing the work.
- Get two to three written estimates before choosing a contractor.
- Get references on the contractor and contact them.
- 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 are to 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 as an incentive to enter into a contract for exterior repair. If the insurer denies the claim in whole or in part, you have the right to cancel the written contract within three days of the notice under Wisconsin's Residential Contractor law (Wis. Stat. s. 100.65).
- Get lien waivers from anyone that you pay for home repairs.
- Never pay with cash or checks made out to cash.
- If you have problems with the work performed, contact the Bureau of Consumer Protection to learn more about Wisconsin's Home Improvement laws (Wis. Adm. Code ch. ATCP 110)

Transient Crews

Do not let strangers into your home – not even to use the bathroom or get a drink of water.

In the wake of major storms, "storm chasers" travel to hard-hit communities and offer seemingly irresistible deals for construction or repair help. They pressure homeowners for upfront payments or increase prices arbitrarily as they work. These teams come and go from an area without a trace, leaving consumers empty-handed and with no recourse for any work they have not completed or any damage they have done to a homeowner's property.

Protect Yourself

- Check their credentials by looking up the company's number in the phone book and call to check on the identity of the seller.
- Contact the police or sheriff 's department to verify that 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 to do a job without your authorization.

Complaint Letters

If you are dissatisfied with the purchase of a product or service, contact the business and let them know about the issue, while providing them an opportunity to resolve the matter.

If your first contact by phone or in person is not successful, you may achieve more satisfactory results by sending the company a complaint letter.

Complaint writing tips

- Keep the letter brief and to the point, while including all pertinent facts (date and place of transaction, name of product, and serial number).
- State the problem and indicate what you believe would be a fair and just settlement of the problem.
- Include your name, address, home and work phone numbers, and email address.
- Send copies of important documents, not originals.
- Sending documents through certified mail is recommended.
- Give the business a deadline for their response, but be reasonable.
- Provide the names of offices, agencies, or associations you intend to go to for help if your problem is not resolved.
- Avoid writing a sarcastic, threatening, or angry letter – it may lessen your chances of getting the complaint resolved.
- Keep copies of your letter and all related documents and information.

How to File a Complaint

Consumer complaints may be filed with the Bureau of Consumer Protection at any time.

- All complaints must be received in writing.
- You may submit a complaint online, in person, or by mail or email.
- Submit copies (**not originals**) when you have documents to support your complaint.
- General and topic-specific complaint forms are available online or can be mailed upon request. Contact us if you need a form mailed to you.
- Contact the Bureau of Consumer Protection if you have questions or need further assistance.

What Happens to Your Complaint

Complaints are handled in the order received and are assigned to a staff person who will contact the business about your complaint.

The staff person will notify you:

- When your complaint is assigned a file number and their contact information.
- If we forward your complaint to another agency.
- When we get feedback from the business.
- If the business refuses to respond.
- If we are unable to locate a valid address on the business.

Our correspondence with the business may include potential violations of state consumer laws. In some situations, we may:

- Issue a formal warning notice to the business.
- Recommend the case to the Department of Justice or to a district attorney for prosecution at their discretion.

If the business does not settle the complaint to your satisfaction, you might consider:

- Discussing your complaint with an attorney.
- Taking action in small claims court if that court has the power to hear your complaint.

Judgments and money awards can only be made by the court system. The Bureau of Consumer Protection strives to mediate a resolution informally before a situation goes to court. However, you can take someone to court without going through the Bureau of Consumer Protection first, and you can always take someone to court if the Bureau of Consumer Protection is unable to assist to your satisfaction.

Small Claims Court

Any individual or corporation doing business in Wisconsin can sue or be sued in small claims court. Wisconsin Statutes Chapter 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 it is your right to hire an attorney.

Necessary forms

- 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 tell you which courthouse to file the completed forms with.
- Filing fees differ from county to county.

Serving the paperwork

Copies of the filed forms must be "served on" or delivered to the defendant. Check with the county where you filed to determine acceptable delivery options.

Going to court

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 both parties appear at this first conference and cannot reach agreement, the matter will be scheduled for a hearing before a commissioner. In some highly populated counties, such as Milwaukee County, a court commissioner may informally hear and decide your case on the first court date.

If you are not satisfied with what is done at the informal conference or by a court commissioner, you maintain an absolute right to have your case heard by a circuit court judge in a full trial.

Judgment settlement

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

Eldercare Locator

U.S. Administration on Aging
1-800-677-1116
eldercare.gov

Information on local services for the elderly.

Funeral Planning

Federal Trade Commission (FTC)
600 Pennsylvania Avenue NW
Washington, DC 20580
202-326-2222
ftc.gov

The FTC offers a detailed funeral planning guide titled: "Shopping for Funeral Services"

Insurance

Wisconsin Office of the Commissioner of Insurance (OCI)
125 S Webster St.
PO Box 7873
Madison, WI 53707-7873
608-266-3585
1-800-236-8517
oci.wi.gov

To file a complaint against your insurance company or agent, contact OCI.

Medicare & Medicaid

Medicare Contact Center Operations
PO Box 1270
Lawrence, KS 66044
1-800-633-4227
medicare.gov

access.wisconsin.gov is a website for low-income seniors and people with disabilities wanting to reduce their prescription drug costs.

Medigap Hotline at 1-800-242-1060 answers Medicare-related questions for Wisconsin residents.

Unclaimed Property

Wisconsin Department of Revenue
PO Box 8982
Madison, WI 53708-8982
608-264-4594
revenue.wi.gov/ucp/
Email: DORUnclaimedProperty@revenue.wi.gov

Find out whether you have any unclaimed funds from financial institutions, life insurance companies, etc.

Bureau of Consumer Protection Contacts

Department of Agriculture, Trade and Consumer Protection
Bureau of Consumer Protection

2811 Agriculture Dr.
PO Box 8911
Madison, WI 53708-8911
1-800-422-7128
datcp.wi.gov
Email: DATCPHotline@wi.gov

Wisconsin Do Not Call

2811 Agriculture Dr.
PO Box 8911
Madison, WI 53708-8911
Email: WINoCall@wi.gov
Consumer sign up for the Wisconsin Do Not Call Registry:
1-888-382-1222
NoCall.Wisconsin.gov

The Bureau provides services to inform, educate and protect the public on a number of other consumer issues including:

- Landlord/tenant
- Motor vehicle repairs
- Product safety
- Fitness and weight loss centers
- Food service plans
- Manufactured housing communities
- Direct marketing
- Unfair, deceptive, misleading advertising
- Residential contractors

Department of Agriculture, Trade and Consumer Protection

Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison, WI 53708-8911

datcp.wi.gov
DATCPHotline@wi.gov
1-800-422-7128

tcp_cic_170.indd (rev. 01/20)

Phishing, Vishing, Smishing…

Phishing

"Urgent! Your account has been suspended. Please visit this link to update your information and reinstate your account." Have you ever received an email like this, from a company with whom you do not have an account? If so, you have been the target of a "phishing" scam.

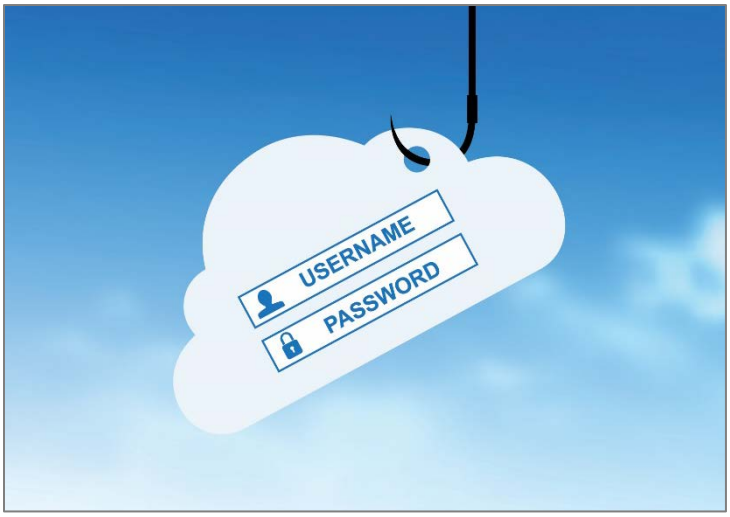
Do not click on any link in an email that may be phishy.

The term "Phishing," was intentionally coined as a play on "fishing." Fishing is exactly what the scam artists are doing – throwing you deceptive bait to see if you will bite and give up your personal information. Once they have that, scammers can make unauthorized charges to your bank account or credit card, or even open fraudulent accounts in your name.

Internet scammers are now well-known for sending mass emails (spam) or internet pop-up messages which seem to be from a friend or from a business or organization that you deal with – such as a bank, credit card company, or even a government agency. The message may ask you to "update," "validate," or "confirm" your account. Some phishing emails threaten serious consequences if you do not respond. The message will ask you to click on a link or call a phone number. It is very easy for con-artists to take logos or web images and recreate them to look and feel very legitimate or familiar. As real as the websites may seem, they are not legitimate.

Malicious links

Do not click on any link in an email that may be phishy – scammers can display an impersonated organization's actual web address in a link while still sending you to a bogus site. Open a new browser and type in a web address you know to be correct, or call the organization using the phone number published in a directory. Since many consumers have started to catch on to the standard scams, fraudsters have become more sophisticated.



A link or attachment may lead to malicious software, known as "malware," being installed onto your computer. Malware may allow a scammer to access your personal files, log your keystrokes to capture your passwords and account numbers, or even take control of your computer to send phishing emails to others.

Cyber imposters

Fraudsters may even use your identity to scam someone you know. If scammers are able to gain access to your email or social media accounts, they can contact your friends and family while posing as you. The scammers will change your password immediately upon accessing your account, thereby locking you out and cutting you off from all your contacts.

They can then send urgent messages to all of your contacts, telling them that you have run into trouble, or are stranded abroad and need money wired as soon as possible. By the time you are able to get the word out that you are okay, a well-intentioned friend or family member may have already wired money abroad. Also, many computer viruses are spread through compromised email contact lists. A familiar "from" address in an email is no guarantee of trustworthiness.

Spoofing

Spoofing commonly occurs when scammers use electronic devices to disguise their true identities or to hide the origins of their messages while phishing. In other words, the scammer will post a name or number on your email, phone caller ID, text message, or even internet URL as being from a person or place of business that you know and trust. Do not be fooled. The scammer behind the fake ID could be in another state or country using false names and titles that are impossible to trace.

Vishing & Smishing

After consumers started catching on to the phishing scams through email, scammers turned to a new method of targeting their victims by phone: vishing. **Vishing** is very similar to phishing, but scammers use telephone calls (either live or pre-recorded "robo-calls") instead of emails to try and lure people into giving up personal information. Vishers often rely on the use of posing as a local bank, credit union or other legitimate business that you might be inclined to trust or patronize.

Since scammers can "spoof" any name and phone number that they want, the scammer can easily make a familiar or trusted business name appear on your caller ID. For example, a recorded message claims that the consumer's bank account has been compromised. When the consumer calls back, he/she speaks with a live person posing as a bank employee, who convinces the consumer that the only way to protect precious bank account information from criminals is to give the "bank employee" his/her personal information.

If you ever receive a vishing call from someone claiming to be an employee of your bank, credit card company, or any other business – hang up. Then call the actual business immediately to report the incident. Be sure to call using only a reliable telephone number obtained from your local phone book or from your paperwork with that business.

When the scam uses text messaging rather than a phone call or email, the scam technique is known as **smishing**. Typically, smishing text messages come from a "50000" number, instead of showing a typical phone number. This indicates that the message was sent from an email address, and not from an actual phone.

As with phishing and vishing scams, **you should not respond** to a smishing text message. If it seems to be a message from your bank or other business you are familiar with, contact that business using a reliable telephone number from your local phone book or from your paperwork with that business.

If you receive a phishing email, ask yourself:

1. **Have I ever done business with this company?** If yes, still be cautious before clicking any links. If no, do not click any links and delete the email.
2. **Are there any attachments with the email?** If yes, do not click on them. If you believe the email and attachment are legitimate, contact the sender first to verify the contents and security of the attachment.
3. **Does the email request any personal information (such as Social Security number, Medicare card number, date of birth, credit card numbers, bank account numbers, or passwords)?** If so, do not reply. Delete the email.
4. **Does the email contain grammatical errors and awkward sentences?** If so, do not reply. Many times phishers are from foreign countries. The grammatical errors are a red flag that the email is not from a professional, reputable and, most importantly, legitimate business.
5. **Still not sure about the email's legitimacy?** If you still think that the email may be from a legitimate company that you have done business with (such as your bank or a government agency), look up a telephone number for that business or agency. Use a local, trusted phone directory or paperwork you have from the business (such as a bank statement or the back of a credit or debit card). Call the business or agency directly and ask them if they sent you the email.

What to do if you fall victim

If you believe you have fallen for a phishing, vishing or smishing scam, do not panic. There are simple steps you can take to protect your personal information.

1. **Check your free annual credit report regularly.** Obtain your credit report **FREE** from each of the three (3) major credit reporting agencies each year. Checking your

report regularly is one of the best ways to protect against ID theft. We recommend you check one report once every four (4) months. You can get your free credit report from any of the three (3) – Equifax, Experian and TransUnion – by calling 1-877-322-8228, or online at www.annualcreditreport.com. Review your report for any errors or possible fraud. If you find errors or possible fraud, contact the credit reporting agency and dispute your claim. Our office may also be able to assist you with this process.

2. **Place a fraud alert on your credit report.** A fraud alert is a free service you can request from each of the three major credit reporting bureaus. The alert lets potential creditors know that you may be the victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures in order to protect you. It stays on your report for one year and can be renewed. You can request the fraud alert by calling one of the three major credit reporting bureaus, they will notify the other two major credit reporting bureaus:

   Equifax (CSC Credit Service)
   PO Box 105788
   Atlanta, GA 30348-5069
   1-800-685-1111
   1-888-298--0045
   www.equifax.com

   Experian
   PO Box 9554
   Allen, TX 75013
   1-888-397-3742
   www.experian.com/fraud

   TransUnion
   PO Box 2000
   Chester, PA 19016
   1-888-909-8872
   www.transunion.com

3. **Close any financial accounts that may have been compromised.** If you gave out a credit card number or checking account number, call your financial institution and ask that the account be closed and reopened under a new account number. Ask your bank if you can place a password on your accounts. Some institutions may offer to monitor your account, but we highly recommend you completely close the compromised account.

   If you provided your driver's license number, contact the Division of Motor Vehicles. Phone them at (608) 264-7447 or find them online at

   www.dot.state.wi.us.

4. **To help reduce telemarketing calls, sign up for the Do Not Call Registry.** Register your home and mobile residential numbers on the Wisconsin Do Not Call Registry at no cost by visiting: NoCall.Wisconsin.gov or by calling 1-888-382-1222. You must call from the phone number you wish to register. Telemarketers have up to 31 days from the date you register to stop calling you.

5. **If you become a victim of identity theft, contact the Bureau of Consumer Protection.** You can call 1-800-422-7128 or email us at:

   DATCPWisconsinPrivacy@wi.gov

For more information, visit the website at:

www.datcp.wi.gov

For more information or to file a complaint, visit our website or contact:

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

Email: DATCPHotline@ wisconsin.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

Phishing402 (rev 11/19)

Imposter Scams

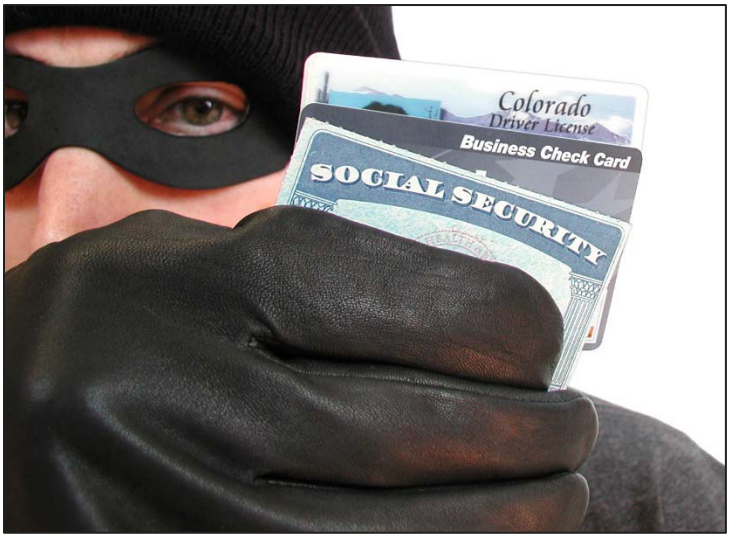
Beware! Imposters are everywhere! When the phone rings, do you know who is calling before you answer or who sent the mail you just opened? When at your computer or on your smart phone, do you know who sent the email in your inbox? Do you know who created that pop up message on your screen? All of these methods, and many more, are being used by scammers who are not what they may seem to be.

The best defense against imposter scams is to not respond.

Signs of an Imposter Scam

Here are some common indicators you are dealing with an imposter:

- **Requests for personal information.** Examples include: date of birth, social security number, Medicare ID number, credit card numbers, or bank account numbers.
- **Requests for payment of any kind.** No contest, prize or grant recipients have to make payment to receive their winnings or award.
- **Requests for payment by wiring money or pre-paid debit cards**. Providing money through either of these is the same as giving someone cash and it is not likely it can be traced or retrieved once given.
- **Threats and urgency.** The more threatening the call – you'll be arrested, have to go to court, have your credit ruined – the more likely it is from an imposter. Calls requiring urgent action from someone you do not know are likely made by imposters.
- **Requests for secrecy.** This is especially true for appeals for financial assistance from relatives who say "Don't tell my mom and dad." Also for calls about winning a prize where you are told by the caller "you can't tell anyone else about it until you have received your winnings."



Imposter Phone Scams

- **IRS or Department of Treasury**. Calls threatening you must pay now for tax violations. **The IRS will not contact you by phone. They would contact you by mail. They will not make threats.**
- **Federal Grant Award.** Do not be fooled by the 202 area code used to look like the call is coming from Washington, D.C. These unsolicited grants are not awarded. In the rare case where someone receives a grant they did not apply for, **no payment is required to receive the grant.**
- **Medicare or Affordable Health Care Act.** The caller claims to be a government representative insisting you provide personal identification information and/or pay a fee or face loss of benefits. **Government agencies will contact you by mail, not by phone. They will not make threats on the phone.**
- **Other Law Enforcement or Government Agency.** The caller may threaten deportation, but for a fee will assist you to get your certification. They hope you will be scared enough to part with money and/or personal identification information. A caller may claim that a foreign dignitary, who needs your help with a money transfer, is "legitimate". **No law**

enforcement or government agency makes these kinds of calls.

- **Lottery or Prize Winner.** The caller says you have won but an administrative fee, shipping, or taxes need to be paid. **You never have to pay for a prize or winnings.**
- **Family Assistance.** Also known as the "Grandparent's Scam". These callers prey on the goodwill and desire to help family. The caller will say they are a family member, usually a younger one, in some kind of trouble needing immediate financial assistance. These scammers will feed off of information you inadvertently give them. **The caller will ask you not to call someone who could verify the legitimacy of the call** ("Don't call mom or dad") and to send money in an untraceable manner.
- **Computer Problems.** The caller claims to be from "Microsoft" or "Google" or another known company and states they have detected a problem with your computer. The caller may tell you to look in a particular place in your computer where you will see many error messages. The caller will tell you this is because of a virus or other problem with your computer. **The error messages you are seeing are completely normal on any properly functioning computer.** These callers will attempt to get you to pay for services, likely via credit card, and to give access to your computer so they can steal personal information and download damaging software known as "malware" that will continue to allow access and even control of your computer. Legitimate companies do not make these kinds of calls. **Never give a caller access to your computer unless you are sure you know who is on the other side of the phone.**
- **Utility shut off.** The caller states you haven't paid your utility bill and someone is on the way over to disconnect your service unless you make an immediate payment to the caller. These calls target small businesses but some consumers report receiving these calls at home. To check if what the caller says is true, **call the number on your billing statement, not the number the caller gives you.**
- "**Spoofed" Numbers.** Technology exists that allows a caller to control what shows up on Caller ID. This is called **"spoofing".** Calls may appear to come from a governmental agency, company or even a neighbor, when the calls are actually coming from outside the country. **If you do not recognize the number on the Caller ID, let the call go to your answering machine or voicemail.** If it is important or a personal call, the caller will leave a message. If you have a question about the message left, call the Consumer Protection Hotline at 1-800-422-7128.

Imposter Mail Scams

Mail scams require a response once you've received the mail. The most common imposter scams are prize scams where you are instructed to call and told you need to make a payment of some sort to receive your winnings. Versions of the phone imposter scams may also come in the mail or through email.

Imposter Computer Scams

- **Email scams.** Email imposter scams may be versions of the imposter phone or mail scams. Often the objective may be to get you to click on a link that will ask you for personal information or to click on an attachment that will download a virus or other malware to your computer.
- **Screen Pop-Ups.** A message will pop up on your screen, usually claiming there is something wrong with your computer and telling you to click on the window for assistance. You will then be given information to contact someone to help you, possibly from a known company like "Microsoft" or "Google". This is a variation on the Computer Problem calls. Often the screen pop-up messages are the result of a virus that has been downloaded to your computer to get you to make contact with them rather than them calling you. Sometimes you may receive a call once this message appears or you click on the pop up window. If an error message appears on your computer, contact someone you know and trust for help. Do not click on pop-up windows reporting a problem with your computer.

- **Online search imposter scams.** When looking for assistance through an online search, be aware that some companies, including scammers, have paid to have their links appear at the top of your search list. It is very easy to think you are talking to a representative of the actual company you want, or are on their website, only to find you are being asked to provide personal information, payment information and/or access to your computer. Check the website address to make sure you are dealing with the real company.
- **Online dating imposter scams.** Online dating makes it easier for a person to misrepresent themselves. Fake or outdated photos may be used, personal histories enhanced or exaggerated, or personal traits fabricated. With traditional dating, it is possible to talk with friends, family members or acquaintances to check a person's reputation. Online dating does not usually make this possible. Once a scammer is confident they have your trust, they will start asking for money. They may tell you they need it to help get money the government owes them, cover the costs of a sudden illness, surgery, a robbery, accident, or job loss. It may be for them or a daughter or son. They may ask for money to cover the cost of travel to finally meet face-to-face. You might get documents from an attorney as "proof" of their genuine intentions along with a promise to pay it back. As real as the relationship seems, it is a scam and you lose the money sent.
- **Social networking website imposter scams.** Treat links in messages on these sites as you would a link in an email message. If it looks suspicious, even if you know the source, it is best to delete it or mark it as junk. Hackers can break into accounts and send messages that look like they are from your friends, but are not. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. Do not trust that a message is really from who it says it is from.

Do Not Respond!

The best defense against all these imposter scam is to not respond.

- **Do not answer the call.** Use your Caller ID. If you do not recognize the number, let it go to your answering machine or voicemail. If you do answer the call, hang up as soon as you realize this is not someone you want to talk with. Talking to these callers or calling them back will likely result in additional contacts from them and other scammers.
- **Delete email from unknown senders.** If you do not know who sent it, do not open it. Sometimes opening an email is enough to tell a scammer that this is a valid address and they will continue to send you email. **If you do not know who sent it, never click on a link or attachment in an email.**
- **Verify your search result.** Before acting on the result of an online search, check to make sure you are dealing with the company you want**. If you do make contact, watch for the signs of a scam.**
- Do not call the verification number you are given. Call the number on a billing statement, found in the phone book or reliable online directory. **Never check to see if something is legit using the number given to you on the call, mailer, email or message.**

For more information or to file a complaint, visit our website or contact:

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

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

ImposterScams214 (rev 8/19)

Your Social Security Number

Social security numbers were originally created for the purpose of tracking earnings and paying benefits. They were never meant to be used by businesses as an identifier, but have taken on that role because everyone has one.

Just about everybody wants your social security number today – schools, phone companies, utility companies, insurance companies, health clubs etc. Many want the number to get your credit rating, to determine whether you pay your bills, and to keep track of you through name and address changes. Some companies use your social security number to develop marketing lists which they can sell to other companies.

Your social security number is a primary target for identity thieves.

Thieves also want your social security number. A stolen wallet containing a social security card lets a criminal quickly set up fraudulent accounts in your name.

The snowballing problem of identity theft is spurring some states to limit the use of social security numbers. In the meantime, the first defense against the fraudulent use of social security numbers is to not give your number to anyone who does not absolutely need it.

Safeguard your social security number

Your social security number is a primary target for identity thieves. The more people who know your social security number, the more susceptible you are to identity theft.

- Do not ever carry your social security card with you.
- Do not carry other cards that may contain your social security number, like a health insurance card or a school identification card.

Who has the right to ask for your number?

While any business can ask for your social security number, there are very few entities that can actually demand it – motor vehicle departments, tax departments and welfare departments, for example. Also, social security numbers are required for transactions involving taxes, so that means banks, brokerages, employers, and the like also have a legitimate need for your social security number.

Most other businesses have no legal right to demand your number. There is no law prohibiting a business from asking for your social security number, but asking for it does not mean you have to give it. Ask if the business will accept an alternative piece of identification. Since some businesses use your social security number to check your credit worthiness, there is a possibility they will refuse to use a different identifier and may refuse to provide whatever product or service you are seeking. But a business may accept your refusal and complete the transaction. If they do not, you might want to consider choosing not to do business with them.

Find out if someone is fraudulently using your social security number

The best way to find out if someone is fraudulently using your social security number is to regularly monitor your credit reports.

Consumers should obtain one free credit report from each of the three credit reporting companies a year. We recommend consumers review their credit report every four months. For example, in January, check your report from TransUnion, in May, check your report from Equifax, and, in September, check your report from Experian. You can order your free credit reports online at: http://www.annualcreditreport.com or by phone, toll free, at 1-877-322-8228.

You should also verify your Social Security Statement once a year from the Social Security Administration. This will determine if someone is fraudulently employed using your social security number. You can request your Social Security Statement online at http://www.ssa.gov or by phone, at 1-800-772-1213.

For more information or to file a complaint, visit our website or contact:

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

Email: DATCPWisconsinPrivacy@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftYourSSN606 (rev 2/19-G)

Tips For Using Public Wi-Fi

Wi-Fi (short for "Wireless Fidelity") is a radio wave-based technology that allows computers, smartphones, and other electronic devices to connect to the internet or to communicate with one another wirelessly.

A number of coffee shops, libraries, airports, hospitals, hotels, fast food restaurants, and other businesses are using Wi-Fi to provide free public access points (or hotspots) that their customers can use to connect wirelessly to the internet. A single hotspot typically has a range of about 65 feet indoors and a greater range outdoors.

Do not stay permanently signed in to accounts.

Accessing the internet using a public Wi-Fi hotspot is convenient and often free for mobile users, but hotspots typically are not secure. If you are not required to enter a password provided by the Wi-Fi host (i.e. coffee shop or hotel) before gaining access to the network, another Wi-Fi user could hack into your electronic device and view your personal information and what you are sending. They could change your passwords and block you out of your own files. They could even use your account to impersonate you and scam the people you care about. So if you are not certain that a network is secure, treat it as if it were unsecure.

How encryption works

In addition to using secure networks, it is best to send sensitive information only to encrypted websites. If you send email, share digital photos and videos, use social networks, or bank online, you are sending personal information over the internet. The information you share is stored on a server – a powerful computer that collects and delivers content. Many websites (such as banking sites) use encryption to protect your information as it travels between your computer and their servers. Encryption is the key to keeping your personal information secure online. Encryption scrambles the information you send over the internet into a code that it is not accessible to others. When

using wireless networks, it is best to send personal information only if it is encrypted – either by an encrypted website or a secure Wi-Fi network. An encrypted website protects **only** the information you send to and from **that site**. A secure wireless network encrypts all the information you send using that network.

How to tell if a website is encrypted

Encrypted websites will have "**https**" at the beginning of the web address (the "s" is for secure). Some websites use encryption only on the sign-in page, but if any part of your session is not encrypted, your entire account could be vulnerable. Look for **https** on every page you visit, not just when you sign in.

Do not assume a Wi-Fi hotspot is secure

Most Wi-Fi hotspots **do not** encrypt the information you send over the internet and are **not** secure. If you use an unsecured network to log on to an encrypted website or a site that uses encryption only on the sign-in page, other users on the network can see what you see and what you send. They could hijack your session and log in as you. New hacking tools, available for free online, make this easy, even for users with limited technical know-how. Your personal information, private

documents, contacts, family photos, and even your log-in credentials could be compromised.

Turn on two-factor authentication if offered

Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized, such as a personal identification number (PIN) or password.

Protect yourself when using public Wi-Fi

- When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted. To ensure security, your entire visit to each site should be encrypted (look for https in the address bar). If you are not sure if you are on a secure page, log out right away.
- Do not stay permanently signed in to accounts. Log out when you are done using any account.
- Do not use the same password on different websites. It could give someone who gains access to one of your accounts access to all of your accounts.
- Many web browsers alert users who unknowingly attempt to visit fraudulent websites or download malicious programs. Pay attention to these warnings and keep your browser and security software up-to-date.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can obtain a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees.
- WEP and WPA are the most common types of Wi-Fi encryption available. WPA encryption protects your information against common hacking programs while WEP may not. WPA2 is the strongest. Use the same precautions as on an unsecured network if you are not certain that you are on a WPA network.
- Installing browser add-ons or plug-ins can also help. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually are not encrypted. They do not protect you on all websites, so remember to look for https in the URL to confirm if a site is secure.
- For more information on using public Wi-Fi hotspots, visit:

  StaySafe Online
  staysafeonline.org

  OnGuardOnline
  onguardonline.gov

  Federal Trade Commission
  ftc.gov

Common Wi-Fi terms

Encryption

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

FTP

A protocol that allows users to copy files between their local system and any system they can reach on the network.

HTTPS – Hypertext Transfer Protocol Secure

HTTPS is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the Internet.

"Man-in-the-middle" attacks

A "man-in-the-middle" attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection – when in fact the entire conversation is being controlled by the attacker. The attacker must be

able to intercept all messages going between the two victims and inject new ones. For example, an attacker within reception range of an unencrypted Wi-Fi access point can insert himself as a man-in-the-middle. Or an attacker can pose as an online bank or merchant, letting victims sign in over a SSL connection, and then the attacker can log onto the real server using the victim's information and steal credit card numbers.

SSL – Secure Sockets Layer

SSL protocol is for securing data communications across computer networks. It establishes a secure session by electronically authenticating each end of an encrypted transmission. It is used by websites whose names begin with https instead of http.

VPN – Virtual Private Network

A Virtual Private Network (VPN) secures and privatizes data across a network, usually the internet, by building an "encrypted tunnel." Data passes through this tunnel, protecting it from anyone who tries to intercept it. Even if the data is intercepted, it is hopelessly scrambled and useless to anyone without the key to decrypt it.

WEP – Wired Equivalent Privacy and WPA/WPA2 – Wi-Fi Protected Access

WEP and WPA are types of security connections that are used to protect home wireless networks. WEP is a security algorithm that was introduced in 1997 to provide confidentiality comparable to that of a traditional wired network. Since 2001, several serious weaknesses in the WEP protocol have been identified, and today a WEP connection can be cracked within minutes. In 2003 WEP was superseded by Wi-Fi Protected Access (WPA). WPA and WPA2 are certification programs that test Wi-Fi product support for IEEE-standard security protocols that can encrypt data sent over the air, from Wi-Fi user to Wi-Fi router.

For more information or to file a complaint, visit our website or contact:
Wisconsin Department of Agriculture, Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Email: DATCPWisconsinPrivacy@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftWi-fiTips659 (rev 11/19)

Creating Strong Passwords

Passwords are the first line of defense in protecting you against cyber criminals (hackers) while conducting online transactions (i.e. banking, paying bills, or making purchases). If hackers gain unauthorized access to your computer, they can view your personal information; impersonate you and send messages to your friends; change your password and block you from accessing your own account; steal your identity; or infect your files with viruses. Therefore, it is vital to pick strong passwords that are different for each of your accounts and to update your passwords regularly.

Update your passwords regularly.

Here are some tips that will help protect your online transactions:

Use a unique password for each of your important accounts like email and online banking

Choosing the same password for each of your online accounts is like using the same key to lock your home, car and office – if a criminal gains access to one, all three are compromised and can lead to identity theft. Do not use the same password for an online newsletter that you use for your email or bank account. It may be less convenient, but picking multiple passwords keeps you safer.

Create a strong password by combining numbers, letters and symbols

Strong passwords are easy to remember but hard to guess. Make your password strong to help keep your information safe. Adding numbers, symbols and mixed-case letters makes it harder for cyber criminals or others to guess your password. Do not use obvious passwords like '123456' or 'password,' and avoid using publicly available information like your phone number or the name of a pet, a child or another familiar person. Likewise, avoid things that can be looked up, such as your birthday or ZIP code.

Longer = stronger. Your passwords should be a minimum of 8 characters, but the longer you can make them, the harder it will be for a thief to crack your codes. While it is best to avoid using real words as part of your password, if you do, you can try substituting characters for some of the letters, e.g. $ for an S, or a zero for an O. Another way would be to insert a string of characters or numbers in the middle of a real word, thus breaking it up into two non-words.

Try using a phrase that only you know

You could start with "**My friends Mary and Jack send me a funny text message every day**" and then use numbers and letters to recreate it into this: **MfM&Jsmaftmed** – a password with many variations that will be hard for cybercriminals to figure out. Another example would be something like **Iam:)2bH!** – this has 9 characters and says "**I am happy to be here!**" Come up with a system to create your own passphrases. That will make it easier to create new passwords as well as help you remember them.

Adding a cell phone number

Sometimes you can add a phone number to your profile to receive a code to reset your password via text message. Having a mobile phone number on your account is one of the easiest and most reliable ways to help keep your account safe.

For example, service providers can use the phone number to challenge those who try to break into your account, and can send you a verification code so you can get into your account if you ever lose access. Your mobile phone is a more secure identification method than your recovery email address or a security question because, unlike the other two, you have physical possession of your mobile phone.

Turn on two-factor authentication if offered

Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.

Choosing a unique security question

If you cannot or do not want to add a phone number to your account, many websites may ask you to choose a question to verify your identity in case you forget your password. If the service you are using allows you to create your own question, try to come up with a question that has an answer only you would know and is not something that you have posted about publicly or shared on social media. Try to find a way to make your answer unique but memorable – so that even if someone guesses the answer, they will not know how to enter it properly.

Set up your password recovery options and keep them up-to-date

If you forget your password or get locked out, you will need a way to get back into your account. Many services will send you an email at a recovery email address if you need to reset your password. Make sure your recovery email address is up-to-date and is an account you can still access, or have it sent by text to your mobile device.

Keep your passwords in a secret place that is not visible

Writing down your passwords is not necessarily a bad idea, but make sure you put those notes in a secure area. Do not leave them in plain sight or easily accessed.

You may want to consider using a password manager. The most basic password managers are like a lockbox or vault in your computer. You can create unique, complex, strong passwords, even ones you would never remember, for each website you need to log in to. The manager remembers and stores them so when you need them, the manager enters your login information, including the password, so you can safely log in.

These passwords are stored in the manager, secured by one master password that you do need to remember. This facilitates creating strong passwords that you do not have to remember. A much better way to safely store your collection of passwords than writing them down on a piece of paper! You will need to research the various products available to see which one has the right combination of features that will work best for you.

For more information or to file a complaint, visit our website or contact:

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

Email: DATCPWisconsinPrivacy@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftPasswordsCreating658 (rev 9/19)

Identity Theft Protection, Insurance and Credit Monitoring Services

There are many businesses, insurance companies and financial institutions that now offer credit report monitoring services, identity theft protection and identity theft insurance. Some people find it valuable and convenient to pay a company to keep track of their financial accounts, credit reports and personal information. Other people choose to do this on their own for free. Before you pay for a service, do your research to determine if it is something you really need and if it is worth the cost.

A security freeze is the best protection available for financial identity theft.

Consider the following:

- Consumers can check their credit reports for free by calling toll-free at 1-877-322-8228 or online at www.annualcreditreport.com. You are eligible to receive one free disclosure a year from each of the three major credit reporting companies. We recommend that you monitor your credit reports by staggering when you request the reports. For example, in January request a report from Equifax, in April request a report from TransUnion and in August request your report from Experian.
- Consumers can request a fraud alert be placed on their credit reports for free. A fraud alert requires companies to take extra reasonable steps to confirm the customer's identity before proceeding. The fraud alert lasts for one year (or 7 years if a police report is provided) and can be renewed at any time. You only need to contact one of the three credit reporting companies and they will notify the other two on your behalf. For more information, see our Identity Theft Tips and Credit Report Security Freeze brochures.
- The average cost to recover a monetary loss due to identity theft is $503 per victim. Insurance that has a deductible close to or greater than that amount may be considered too pricey.
- Actual financial losses, such as fraudulent credit card charges and withdrawals are typically not covered by identity theft services. Consumers should immediately report lost or stolen cards or fraudulent transactions to their financial institutions to limit liability.
- Consumers can request a security freeze be placed on their credit reports. A security freeze is the best protection available for financial identity theft as it will prevent new lines of credit from being established without your consent. All three credit reporting companies must be contacted directly to request a security freeze be placed on your credit report for free. A Security Freeze is permanent and will remain in place until you remove it. For more information, see our Identity Theft Tips and Credit Report Security Freeze brochures.
- Safeguard your information. Use two-factor authentication if offered. Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.
- The Wisconsin Bureau of Consumer Protection is here to assist consumers in working through the

steps of recovering from identity theft. There is no fee to file an identity theft complaint with our office.

For more information or to file a complaint, visit our website or contact:

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

Email: DATCPWisconsinPrivacy@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftInsurance617 (rev 10/19)

Credit Report Security Freeze

A security freeze can help protect against identity theft by prohibiting the release of any information on the credit report without express authorization, except to those with whom you have an existing account or a collection agency acting on behalf of the existing account, for the purposes of reviewing or collecting the account. A security freeze is designed to prevent an extension of credit, such as a loan or a new credit card, from being approved without consent.

A security freeze can help protect against identity theft.

What do the credit reporting agencies charge?

	Placing a Freeze	Temporary Lift	Freeze Removal
Identity Theft Victim:	FREE	FREE	FREE
Non-Victim:	FREE	FREE	FREE

Wisconsin consumers can place a security freeze on their credit reports for free. Parents and legal guardians can also place a security freeze on the credit report of a child or other protected individual.

To place a security freeze contact each of the three credit reporting agencies directly. You can request a security freeze online, by phone, or by sending a written request by mail.

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze

Equifax Info. Services LLC
PO Box 105788
Atlanta, GA 30348-5069
1-800-685-1111
1-888-298-0045
https://www.freeze.equifax.com

TransUnion
PO Box 2000
Chester, PA 19016
1-888-909-8872
https://www.transunion.com/credit-freeze

Written confirmation of the security freeze will be sent to you within 5 business days of the freeze being placed. It will include a personal identification number (PIN), a copy of your consumer's rights, and instructions for removing the security freeze or authorizing the release of your credit report for a specific period of time.

Removing or temporarily lifting the freeze from your credit report:

When you request a security freeze for your credit report, you will be provided a personal identification number (PIN) to use if you choose to remove the security freeze or authorize the release of your credit report for a specific period of time. Be sure to keep your personal identification number (PIN) in a

secure place for use when needed. To remove your freeze either permanently or temporarily, you must contact the credit reporting agency and provide all of the following:

- The personal identification number (PIN).
- Proper identification with a current address to verify your identity.
- The period of time for which the report shall be made available.

What is the difference between a fraud alert and a freeze?

A fraud alert is a special message on a credit file that states the consumer is or may be a potential identity theft victim. It requires businesses to take extra reasonable steps to verify the identity of the applicant before issuing the line of credit or service. A fraud alert can also slow down your ability to get new credit. It should not stop you from using your existing credit cards or other accounts.

How long does it take for a security freeze to be in effect?

Credit reporting agencies must place the freeze no later than one day after receiving a request by phone or online. Agencies have three days to place the freeze after receiving a written request.

How long does it take for a security freeze to be lifted?

Credit reporting agencies must lift a freeze no later than one hour after receiving a request by phone or online. Agencies have three days to lift the freeze after receiving a written request.

Can I open new credit accounts if my files are frozen?

Yes. If you want to open a new credit account or get a new loan, you can lift the freeze on your credit file. After you request a freeze, each of the credit reporting agencies will send you a Personal Identification Number (PIN). You will also get instructions on how to lift the freeze. A lift period can be specified for a certain amount of time. You can lift the freeze by phone, online, or by mail using the PIN.

What will a creditor who requests my file see if it is frozen?

A creditor will see a message or a code indicating that the file is frozen.

Can a creditor get my credit score if my file is frozen?

No. A creditor who requests your file from one of the three credit reporting agencies will only get a message or a code indicating that the file is frozen.

Can I order my own credit report if my file is frozen?

Yes.

Can anyone see my credit file if it is frozen?

When you have a security freeze on your credit file, certain entities still have access to it. Your report can still be released to your existing creditors or to collection agencies acting on their behalf. They can use it to review or collect on your account. Other creditors may also use your information to make offers of credit- unless you opt out of receiving such offers. Government agencies may have access for collecting child support payments or taxes or for investigating Medicare fraud. Government agencies may also have access in response to a court or administrative order, a subpoena, or a search warrant.

Do I have to freeze my file with all three credit reporting agencies?

Yes. Different credit issuers may use different credit reporting agencies. If you want to stop your credit file from being viewed, you need to freeze it with Equifax, Experian and TransUnion.

Will a freeze lower my credit score?

No.

Can an employer or landlord do a background check on me if I have a freeze on my credit file?

Yes, the security freeze does not apply to anyone using the information for employment, tenant, or background screening purposes.

Does freezing my file mean that I will not receive pre-approved credit offers?

No. You can stop pre-approved credit offers by calling 888-5OPTOUT (888-567-8688). You can also do this online at www.optoutprescreen.com. This will stop most of the offers that go through the credit reporting agencies. You have the option to opt-out for 5 years or permanently.

Can I request a temporary lift with only one credit reporting agency?

Yes. You can determine what credit reporting agency your new creditor uses and request a lift from that agency only. The desired credit reporting agency assigned a unique personal identification number (PIN) when the freeze was placed. You wil be required to provide this PIN to the credit reporting agency to temporarily lift the freeze. A lift period can be specified for a certain amount of time. This method will provide added protection, as the freeze will still be in place with the other two credit reporting agencies.

Can I request a temporary lift for a potential creditor?

Yes. You can grant a creditor one-time access to your credit report. Determine what credit reporting agency your new creditor uses and request a single-use personal identification number (PIN) from that agency. Your creditor will be required to provide this PIN to the credit reporting agency to view your credit report. This method will provide added protection, as the creditor is the only one that will have access to your credit report.

Why when placing a freeze on my credit report would a credit reporting agency require me to photocopy my Social Security Card and/or Driver's License and fax or mail it to them?

The credit reporting agency is attempting to collect your information for the purpose of updating your credit report and authenticating your identity. Make sure all of your important documents, such as your Driver's License have been updated with the most current information.

Can I place a security freeze for a child or protected individual?

Yes, a parent or legal guardian may freeze the credit record of a child or protected individual.

If your child already has a credit report in their name, one of three things has happened. You have applied for credit in their names and applications were approved. You have added them as authorized users or joint accounts holders on one or more of your accounts. Or, someone has fraudulently used their information to apply for credit and the child is already an identity theft victim.

If you suspect your child may be the victim of identity theft, first contact the credit reporting agencies directly and request they do a **manual search** using only the child's social security number. If a file is found, you will be able to obtain a copy to review it for inaccurate or fraudulent information. The credit reporting agencies may require the child's complete name, address, date of birth and a copy of their social security card or birth certificate. As a parent or legal guardian you may also be required to send proof of your identity, guardianship or Power of Attorney.

For more information or to file a complaint, visit our website or contact:

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

Email: DATCPWisconsinPrivacy@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftCreditReportFreeze632 (rev 9/18)

What is Personal Information?

Any combination of the following information can be enough for identity theft to occur:

- Name
- Address
- Phone Number
- Email Address
- ATM Pin
- Date of Birth
- Social Security Number
- Mothers Maiden Name
- Financial Account Numbers

The basics of safeguarding your information

Guard your social security number

Do not carry your Social Security card with you and do not ever use your social security number as a PIN or password. Limit the number of identification cards your carry.

Shred, shred, shred

Shred bills, bank statements, receipts, medical billings, credit card offers, and any other items that contain personal or financial information.

Protect your mail

If you are going to be out of town have the post office hold your mail. Place outgoing mail in an official mailbox not your own.

Never give out your personal information

Legitimate companies or agencies do not call or email asking for personal information. Never give out personal information unless you initiated the contact.

Sign up for the Do Not Call Registry

Register your home and mobile residential numbers on the Wisconsin Do Not Call Registry at no cost by visiting www.donotcall.gov or by calling 1-888-382-1222; you must call from the phone number you wish to register.

Keep a list of all financial accounts

Keep a list of all credit card and bank account numbers, phone numbers, and expiration dates. This information as well as other sensitive documents should be kept in a safe place, such as a safe.

Stop pre-approved credit card offers

Stop pre-approved credit card offers by calling 1-888-567-8688 or visiting the Opt Out website at www.optoutprescreen.com.

Check your bills and bank statements

Look at your statements as soon as you get them to see if there are any unauthorized charges or inaccuracies. If there are, report them right away.

Pay attention to internet security

Make certain you have a firewall and updated virus and spyware protection on your computer. Check your browser security settings to make certain that they are not too low.

Use two-factor authentication if offered

Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.

Check your credit report regularly

Obtain your credit report FREE from each of the three major credit reporting agencies each year. You can get your free credit report from Equifax, Experian, and TransUnion by calling 1-877-322-8228 or online at www.annualcreditreport.com.

What to do if it happens to you

Contact your bank

Let your bank know that your identity has been stolen even if the thief has not used your bank accounts or ATM/debit card. Consider closing and reopening new accounts with new numbers and obtaining a new ATM/debit card with a new PIN. In addition, you may want to ask your bank if you can place a password on your accounts.

Contact your creditors

If an identity thief has opened a new account or credit card in your name contact the creditor to close the account and explain what happened as soon as possible.

Report the theft to the police

File a police report with your local police department even if the theft might have occurred at some other place. Be sure to obtain a copy of the report for yourself. It can be a vital tool to working through recovering from the identity theft.

Put a Fraud Alert on your credit report

A fraud alert is a notation that requires a business to take extra reasonable steps to verify a person's identity before issuing a line of credit or offering services. The fraud alert will be active for one year and can be renewed. You only need to contact one of the three agencies below and they will notify the other two on your behalf.

Put a Security Freeze on your credit report

A freeze is stronger than a fraud alert because it remains in place until you release it and requires that you be alerted if an account in your name is requested. The freeze must be requested by contacting each of the three credit reporting agencies directly.

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
PO Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax Information Services LLC
PO Box 105788
Atlanta, GA 30348-5069
1-800-685-1111
1-888-298-0045
www.equifax.com

File an identity theft complaint with the Bureau of Consumer Protection

We can help with the steps needed to resolve problems caused by identity theft. File an identity theft complaint by calling and requesting a complaint form at 1-800-422-7128 or obtain one online at www.datcp.wi.gov.

Contact the Division of Motor Vehicles if your driver's license or ID card is stolen

WI Department of Transportation
PO Box 7995
Madison, WI 53707
(608) 264-7447
dot.wisconsin.gov

Consider enrolling in the free DMV service called e-notification. E-notification is an electronic service that will send you email or text notifications when activities occur on your account.

wisconsindmv.gov/enotify

Ask the DMV to place a notation on your driving record so that DMV and law enforcement will require additional identification documents when you conduct business with them.

Contact the Postal Inspector if your mail was stolen or if an identity thief used a false address

Contact the nearest Postal Inspector by calling the Postal Service at 1-800-275-8777.

You can also file a mail theft complaint online at https://postalinspectors.uspis.gov.

If a debt collector contacts you

If a debt collector calls, explain that you are the victim of identity theft and that the bill they are trying to collect is fraudulent. Ask for the **steps if you are accused of a crime committed in your name.**

Contact the arresting or citing law enforcement agency to inform them of the situation. You may be required to file a petition with the court to request and prove your innocence. Once law enforcement or a judge conclude that you were not the person who committed the crime, you will be given a Certificate of Clearance that you will need to keep with you at all times.

In some cases, criminal identify theft may best be handled by contacting a private attorney to assist with working through the legal process. The Statewide Lawyer Referral Services Hotline can help you find affordable representation in your area. They can be reached at 1-800-362-9082.

For more information or to file a complaint, visit our website or contact:

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

Email: DATCPWisconsinPrivacy@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftConsumerTips636 Rev 6/19

Bureau of Consumer Protection

Identity Theft

Consumer Tips

Computer Protection Tips

We use computers for everything. BUT….what happens when your computer is hacked? Here are some simple, yet very important steps you can take to help prevent hackers from accessing your computer and personal information.

Use strong passwords.

- **Back up your information often.** You can save your data to a CD, DVD, USB device or an external hard drive. That way, if your computer ever crashes or is hacked, you will not lose all of your information.
- **Never give someone remote access to your computer.** If you receive a call from someone claiming to be from Microsoft or any other company stating you have a virus or that they can fix other issues on your computer, hang up immediately. Scammers will try to convince you to pay for unnecessary services and get access to your computer to obtain personal information or install malicious software.
- **Update your operating system regularly.** Computer operating systems are periodically updated to stay current with technology requirements and to fix weak spots that may be targeted by hackers. Install updates to make sure your computer has the latest version. Often there are settings in your operating system to make these updates automatic.
- **Use strong passwords and change them often.** Do not use the same password for multiple accounts. Use passwords that contain upper and lower case letters, numbers, and symbols. Change your password every three months and do not reuse passwords. This is especially true for passwords that are used to access your email and bank accounts.
- **Use two-factor authentication.** Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.

- **Do not click on pop-ups.** Pop-up windows on the internet are quick advertising tools, but beware of “too good to be true” offers. Not only can these pop-ups slow your computer and internet speed down, but by clicking on these you can accidentally sign up for unauthorized services. Set your browser’s information bar to not allow pop-ups.
- **Be careful what you download.** Some of the most destructive viruses have been hidden in internet programs and applications or e-mail attachments. Download only from a trusted source. As for e-mails, never click on links or attachments if you do not recognize the sender. Even if you do know the sender, beware! It is possible their computer was hacked and is sending out infected e-mails. Those emails may also be very well disguised to look like often used financial institutions or retail websites, sent to phish for your personal information.
- **Do not send sensitive or private information via email.** Email is not usually encrypted, or in other words not in a “secret

code," and can be intercepted and read by hackers.

- **Use antivirus software and set it to update itself daily.** There are many commercial products that can help you protect your computer from various viruses. Most virus protection software has a feature that will scan downloaded files automatically and some will even scan incoming emails by default.
- **Avoid installing unnecessary, unfamiliar, or untested software.** This includes games, toolbars or screensavers that could leave your computer open to attacks. Spyware and viruses are often installed by downloading unfamiliar programs. When you install software, choose a program that is not piggybacking other toolbars or software onto the installation. Look for automatically checked box items in the agreement page giving your permission to install these other items.
- **Use a personal firewall.** A firewall acts as a barrier between you and the internet. It helps keep hackers out and prevents malicious software from sending your personal information to criminals. There are free and retail versions available that come in both software and hardware.
- **Be careful of wireless networks.** For your home network, make sure your router is password protected. For public wireless access (such as at restaurants, libraries or cafes), be aware if the network is unsecured. Cyber criminals take advantage of unsafe networks to hack into your computer and access your personal data.
- **Turn your computer off when not in use.** Leaving your computer on and unattended could leave it open for an attack by hackers. Protect your computer, and save energy by turning your computer off when you are not using it.
- **Dispose of your old computer safely.** Make sure all personal data is removed by the wiping or physical destruction of your computer's hard drive.

If your computer has been hacked and you feel your safety is in jeopardy, or think that the hacker is someone you know, you should call your local police.

Contact a trusted, local computer professional to remove any malicious software that may have been installed.

Technology continues to change and evolve. You may not be able to prevent all hacking, but you can help equip yourself with the tools and knowledge to protect your computer from cyber criminals.

You may also find more helpful tips in our publication "Social Networking."

For more information or to file a complaint, visit our website or contact:

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

Email: DATCPWisconsinPrivacy@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftComputerProtection643 (rev 10/18)

Free Credit Reports

A credit report contains information on where you live, how you pay your bills, and whether you have been sued, arrested, or filed for bankruptcy. Consumer reporting companies sell the information in your report to creditors, insurers, employers, and other businesses that use it to evaluate your applications for credit, insurance, employment, or renting a home. The three nationwide consumer reporting companies are Equifax, Experian, and TransUnion.

Most frequently asked questions and the answers about free credit reports:

Q: How do I order my free reports?

A: There are three authorized ways to order – online at www.annualcreditreport.com, by calling 877-322-8228, or by completing the Annual Credit Report Request Form (forms can be printed from www.ftc.gov/credit). Do not contact the companies individually for your free credit report.

You may order your reports from one, two or all three nationwide consumer reporting companies at the same time. The law allows you to order one free copy from each of the nationwide consumer reporting companies every 12 months.

A warning about other websites – Only one website is authorized to fill orders for the free annual credit report you are entitled to under the law – www.annualcreditreport.com. Other websites claim that they offer "free credit reports," "free credit scores," or "free credit monitoring" are not part of the legally mandated free annual credit report program. In some cases, the "free" product comes with strings attached. For example, some sites sign you up for a "free" service that converts to one you have to pay for after a trial period. If you do not cancel during the trial period, you may be agreeing to let the company start charging fees to your credit card.

Some of these websites use terms like "free report" in their names; others have addresses that purposely misspell annualcreditreport.com in hope that you

mistype the name of the official site; still others advertise so that they appear first in search engines when a person searches for the official site. Some of these sites direct you to other sites that try to sell you something or collect your personal information.

Annualcreditreport.com and the nationwide consumer reporting companies will not send you an email asking for your personal information. If you get an email, see a pop-up, or get a phone call from someone claiming to be from annualcreditreport.com or any of the three nationwide credit reporting companies, do not reply or click on any link in the message. It is probably a scam.

Q: What information do I have to provide to get my free report?

A: You will need to provide your name, address, Social Security number, and date of birth. If you have moved in the last two years, you may have to provide your previous address. To maintain the security of your file, each nationwide consumer reporting company may ask you for information that only you would know, like the amount of your monthly mortgage payment. Each company may ask you for different questions because the information each has in your file may come from different sources. Requests for further information will be made by mail and not by email or telephone.

If you get an email or see a pop-up ad claiming it is from www.annualcreditreport.com or any of the three nationwide consumer reporting companies, do not reply or click on any link in the message – it is probably a scam. Forward any email that claims to be from www.annualcreditreport.com or any of three consumer reporting companies to the FTC's database of deceptive spam at spam@uce.gov.

Q: Why would I want to get a copy of my credit report?

A: You may want to review your credit report:

- To make sure the information is accurate, complete, and up-to-date.
- Because the information it contains may affect your applications and/or costs for loans, credit, insurance, employment, or renting a home.
- To help guard against identity theft. Identity theft is when someone uses your personal information – like your name, your Social Security number, or your credit card number – to commit fraud. Identity thieves may use your information to open a new credit card account in your name. When they do not pay the bills the delinquent account is reported on your credit report. Inaccurate information like that could affect your ability to get credit, insurance, or even a job.

Q: How long does it take to get my report after I order it?

A: You should be able to access online requests immediately. When ordered by calling toll-free

1-877-322-8228, your report will be mailed within 15 days. When mailing in the Annual Credit Report Request Form, your report will be mailed to you within 15 days of receipt.

It may take longer to receive your report if the nationwide consumer reporting company requests more information to verify your identity before processing.

There may be times when the nationwide consumer reporting companies receive an extraordinary volume of requests. If that happens, you may be asked to resubmit your request or be told that your report will be mailed sometime after 15 days from your request. The nationwide consumer reporting companies will inform you when delays occur.

Q: Are there any other situations where I might be eligible for a free report?

A: Under federal law, you are entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft. Otherwise, a consumer reporting company may charge you for another copy of your report within a 12-month period.

Q: Can I purchase additional credit report copies?

A: Yes, by contacting each reporting company:

Equifax Information Services LLC
PO Box 740241
Atlanta, GA 30374
800-685-1111
www.equifax.com

Experian Info Solutions Inc.
PO Box 2002
Allen, TX 75013-0036
888-EXPERIAN
(888-397-3742)
www.experian.com

TransUnion LLC
PO Box 1000
Chester, PA 19016
800-888-4213
www.transunion.com

Q: Should I order a report from each of the three nationwide consumer reporting companies?

A: It is up to you. Because nationwide consumer reporting companies get their information from different sources, the information in your report from one company may not reflect all, or the same,

information in your reports from the other two companies. That is not to say that the information in any of your reports is necessarily inaccurate; it just may be different.

Q: Should I order my reports from all three of the nationwide consumer reporting companies at the same time?

A: You may order one, two, or all three reports at the same time, or you may stagger your requests. It is your choice. Some financial advisors say staggering your requests during a 12-month period may be a good way to keep an eye on the accuracy and completeness of the information in your reports.

Q: What if I find errors – either inaccuracies or incomplete information – in my credit report?

A: Under the Fair Credit Reporting Act, both the consumer reporting company and the information provider (that is, the person, company, or organization that provides information about you to a consumer reporting company) are responsible for correcting inaccurate or incomplete information in your report. To take advantage of all your rights under this law, contact the consumer reporting company and the information provider.

1. Tell the consumer reporting company, in writing, what information you think is inaccurate.

   Consumer reporting companies must investigate the items in question – usually within 30 days – unless they consider your dispute frivolous. They also must forward all the relevant data you provide about the inaccuracy to the organization that provided the information. After the information provider receives notice of a dispute from the consumer reporting company, it must investigate, review the relevant information, and report the results back to the consumer reporting company. If the information provider finds the disputed information is inaccurate, it must notify all three nationwide consumer reporting companies so they can correct the information in your file.

   When the investigation is complete, the consumer reporting company must give you the written results and a free copy of your report if the dispute results in a change. (This free report does not count as your annual free report.) If an item is changed or deleted, the consumer reporting company cannot put the disputed information back in your file unless the information provider verifies that it is accurate and complete. The consumer reporting company also must send you written notice that includes the name, address, and phone number of the information provider.

2. Tell the creditor or other information provider in writing that you dispute an item. Many providers specify an address for disputes. If the provider reports the item to a consumer reporting company, it must include a notice of your dispute. And if you are correct – that is, if the information is found to be inaccurate – the information provider may not report it again.

Q: What can I do if the consumer reporting company or information provider will not correct the information I dispute?

A: If an investigation does not resolve your dispute with the consumer reporting company, you can ask that a statement of the dispute be included in your file and in future reports. You also can ask the consumer reporting company to provide your statement to anyone who received a copy of your report in the recent past. You can expect to pay a fee for this service.

If you tell the information provider that you dispute an item, a notice of your dispute must be included any time the information provider reports the item to a consumer reporting company.

Q: How long can a consumer reporting company report negative information?

A: A consumer reporting company can report most accurate negative information for seven years and bankruptcy information for ten years. There is no time limit on reporting information about criminal convictions; information reported in response to your application for a job that pays more than $75,000 a year; and information reported because you have applied for more than $150,000 worth of credit or life insurance. Information about a lawsuit or an unpaid judgment against you can be reported for seven years or until the statute of limitations runs out, whichever is longer.

Q: Who else can get a copy of my credit report?

A: The Fair Credit Reporting Act specifies who can access your credit report. Creditors, insurers, employers, and other businesses that use the information in your report to evaluate your applications for credit, insurance, employment, or renting a home are among those that have a legal right to access your report.Q: Can my employer get my credit report?

Q: Can my employer get my credit report?

A: An employer can get a copy of your credit report only if you agree. A consumer reporting company cannot provide information about you to your employer, or to a prospective employer, without your written consent.

For more information or to file a complaint, visit our website or contact:

Federal Trade Commission
Bureau of Consumer Protection
Consumer Response Center
600 Pennsylvania Avenue NW
Washington DC 20580
www.ftc.gov
(877) FTC-HELP / (877) 382-4357

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

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

Information taken from Federal Trade Commission website "Free Credit Reports" (http://www.consumer.ftc.gov/articles/0155-free-credit-reports)

CreditReportFree409 (rev 2/19-G)