Identity Theft

Identity theft happens when a thief steals you or your business's personal information in order to use your credit or debit card, take over existing bank accounts, open new accounts, file fake tax returns, rent or buy properties, or do other criminal activities in your name. One of the most common examples of identity theft happens when an individual uses the identifying information on your credit card to make an unauthorized charge.

What Wisconsin Law Prohibit Identity Theft?

Unauthorized use of an individual's identifying information

It is illegal in Wisconsin to use someone's personally identifying information without their permission to:

- Get credit, money, goods, services, employment, or anything of value
- Avoid civil or criminal process or penalty
- Hurt someone's reputation, property, person or estate

"Personally identifying information" is information that can identify a specific individual, and includes a person's:

- Name, address, or telephone number
- Driver's license number
- Social security number
- Employer, employee number, or place of employment
- Taxpayer ID number
- DNA profile
- Mother's maiden name
- Account numbers, passwords, or electronic identifiers that can be used to obtain things of value (e.g. credit card numbers, bank account numbers, ATM passwords)

- Fingerprint, voiceprint, retina iris image, or any other unique physical characteristic

Violation of the law is a felony including up to six years in prison and a $10,000 fine.

Unauthorized use of a business's identifying information

It is similarly unlawful to use a business’s or charity’s account without the consent of that organization to get credit, money, or anything of value. This law stops the unauthorized use of information such as a name, address, employer identification number, bank account number, or credit card number. Violation of the law is a felony including up to six years in prison and a $10,000 fine.

Theft by taking a financial transaction card

It is illegal to take a credit or debit card from someone without the card holder's consent. It is also illegal for a person to have a card for longer than 7 days if they know it has been lost, stolen, or mistakenly delivered to the wrong person. Violation of this law is either a misdemeanor or felony depending on the circumstances.

Fraud against a financial institution

It’s illegal for a person to act as if they represent a bank or other financial organization in order to get someone else’s personal information. This is a felony with a punishment of up to six years in prison and a $10,000 fine.

Harasser acquires personally identifiable information

If a harasser purposely accesses electronic data that has their victim’s personal information in order to make it easier to harass that person, it is a felony with a punishment of up to six years in prison and a $10,000 fine.

Fair Credit Billing Act (FCBA)

The FCBA is a federal law that provides protections to consumers against unfair billing practices. For example, the FCBA says you can only be held responsible for up to $50 if someone uses your credit card without permission. Because of this law, most credit card companies have rules to help protect people from identity theft.

You generally have at least 60 days to dispute a transaction with the card issuer or lender, sometimes longer depending on the type of charge and the policy.

Electronic Fund Transfer Act (EFTA)

EFTA is a federal law that protects you from ATM and debit card fraud. The EFTA applies to many types of electronic fund transfers (EFTs), including transactions made through debit cards, ATMs, person-to-person payments (CashApp, PayPal, Venmo, Zelle, etc.), phones or computers, and direct deposits.

If your debit card is lost or stolen, your level of financial protection depends on how quickly you report it:

When You Report It	Maximum Liability
Withing 2 business days	$50
Between days 3 and 59	Up to $500
After 60 days	No protection — you could lose all the money in the account and owe overdraft fees

Federal Identity Theft Assumption and Deterrence Act is 1998

The law makes it a federal crime to use someone else’s identity to break a federal, state, or local law. Federal agencies like the Secret Service, the FBI, and the Postal Inspection Service investigate these crimes. The U.S. Department of Justice handles the court cases.

How Do I Know If I'm a Victim of Identity Theft?

There are some warning signs that may mean someone has stolen your identity. Keep an eye out for the following:

- Strange charges on your credit card or bank statements that you do not recognize.

- Bills for things you did not buy, accounts you did not open, or medical services you did not use.
- Unexplained withdrawals from your bank account.
- Missing mail or bills that you usually receive—this could mean someone changed your address.
- Calls or letters from debt collectors about accounts you did not open.
- A notice from the IRS saying more than one tax return was filed in your name.
- Being denied credit or a loan for no clear reason, which could mean someone damaged your credit.

If you notice any of these signs, it’s important to act quickly to protect your information and your finances.

What Should I Do if I Believe I'm a Victim of Identity Theft?

Check you credit report

- You can get one free copy of your credit report weekly from each of the three nationwide credit bureaus - Equifax, Experian and TransUnion - online at www.annualcreditreport.com
- You can also submit a paper request form, and get the reports mailed to you, by submitting the following form: https://www.annualcreditreport.com/manualRequestForm.action
- If you discover fraudulent or inaccurate information, have it removed. See our article Disputing a Credit Report for more information.

Contact the company or companies where you believe the fraud occurred

- Ask for the security or fraud department and Let them know you believe someone stole your identity.
- Ask them to provide you with any specific forms for reporting identity theft.
- Ask the company for documentation on the fraudulent accounts, including any application credit card bills, etc. that the identity thief used to open an account or to obtain goods and services in your name.

- Ask the company to stop reporting the fraudulent accounts or transactions to the credit bureaus.
- If applicable, inform them you reported the identity theft to the police and FTC and provide them with copies of the reports.
- Close or freeze the fraudulent account so no new charges are allowed and the identity thief cannot continue to use the account.

Place a fraud alert on your credit cards

A fraud alert, also known as a credit alert, is a free notice placed on your credit file that tells lenders and creditors to take extra steps, such as calling you, to verify your identity before opening new accounts in your name.

Types of Fraud Alerts

Type	Who Can Use It	How Long It Lasts	Cost	Other Benefits
Initial Fraud Alert	Anyone who suspects identity theft	1 year	Free	You can ask for an extra free copy of your credit reports from the three credit bureaus during the year following the placement of the initial fraud alert
Extended Fraud Alert	Victims of conformed identity theft	7 years	Free (with police for FTC report)	You can ask for two free credit reports from the three credit bureaus during the year following the placement of the extended fraud alert, and your name is removed from pre-screened credit card and insurance offers for five years.
Active Duty Alert	For active military members	1 year	Free	Removes you from credit card and insurance offers for two years.

How to Request a Fraud Alert

You only need to contact one of the three major credit bureaus — they'll notify the others. You can place the alerts online (you must create an account), by phone, or by mail:

- Equifax
  - 888-836-6351
  - Mail Fraud Alert Request Form to:
    - Equifax Information Services LLC
      P.O. Box 105069
      Atlanta, GA 30348-5069

Note: When sending the fraud alert request by mail, if you want it to be an extended fraud alert, include a copy of a police report or FTC Identity Theft Report confirming identity theft.

- Experian
  - 888-397-3742
  - Mail a written request to:
    - Experian
      P.O. Box 9554
      Allen, TX 75013
    - **Note:** Written requests should include the following information:
      - Your full name
      - Social Security number
      - Complete addresses for the past two years
      - Date of birth
      - A government issued identification card, such as a driver's license
      - Copy of a utility bill or bank statement
      - Make sure that each copy is easy to read and shows your name, current mailing address and issue date.
      - Proof of Identity Theft (for an extended alert)
- TransUnion
  - 800-916-8800
  - Send a written request that includes your name, address and Social Security number to:
    - TransUnion
      P.O. Box 2000

Chester, PA 19016

What Should I Do If I Know I’m An Identity Theft Victim?

Check your credit reports

- You can get one free copy of your credit report weekly from each of the three nationwide credit bureaus - Equifax, Experian and TransUnion - at www.annualcreditreport.com
- If you discover fraudulent or inaccurate information, have it removed. See our article Disputing a Credit Report for more information.

Close accounts with fraud activity

Contact each business where the identity thief:

- Opened a new account
- Made unauthorized charge
- Changed contact information

Ask them to:

- Close or freeze the account
- Set up new passwords and PINs for existing accounts
    - These should not contain private information such as Social Security numbers or your mother’s maiden name, which could increase the risk for further identity theft.
- Remove fraudulent charges
- Send you confirmation in writing

You may be asked to provide:

- A copy of your police report or FTC Identity Theft Report
- Proof of identity (ID, Social Security card, utility bill)

Important: If mailing documents, do not send the originals. Send copies by certified mail with return receipt requested.

File a report with the Federal Trade Commission (FTC)

- Submit an identity theft report with the Federal Trade Commission at www.identitytheft.gov.
  - Complete the online form or call 1-877-438-4338. Include as many details as possible.
  - Based on the information you enter, IdentityTheft.gov will create an Identity Theft Report and recovery plan.
- Your identity theft report proves to businesses that someone stole your identity. It also guarantees you certain rights.
- If you create an account, the website will walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.
- If you don't create an account, you must print and save your Identity Theft Report and recovery plan right away. Once you leave the page, you won't be able to access or update them.

File a police report

Tell your local police department or the police department in the city where the identity theft happened that someone stole your identity and you need to file a report. Law enforcement may direct you to the file in person, over the phone, or online.

The police may want to see:

- A copy of your FTC Identity Theft Report
- A government-issued ID with a photo
- Proof of your address (mortgage statement, rental agreement, or utilities bill)
- Any other proof you have of the theft (bills, IRS notices, etc.)

Request a copy of the police report for your records. A police report provides you with a document saying you've been a victim. This can help you when requesting a 7-year extended fraud alert on your credit reports.

Place a security freeze on your credit reports

Security freezes (also known as credit freezes) are federally regulated and block anyone from accessing your credit report without your permission. Placing, lifting and removing a security freeze is free.

Check out our All About Security Freezes article to learn how to place and lift a security freeze at each of the three credit bureaus, along with a lot of other information about security freezes.

Additionally, you can place a checking and savings account security freeze by contacting:
Chexsystems
1-800-887-7652
https://www.chexsystems.com/

File a complaint with the Wisconsin Department of Trade, Agriculture, and Consumer Protection (DATCP) Bureau of Consumer Protection

File an identity theft complaint with DATCP when:

- You suffered a financial loss through the fraudulent opening or use of your financial accounts
- You are the victim of tax-related identity theft
- Fraudulent grants or loans are assigned in your name
- Someone used your information to obtain employment or government benefits

To file an identity theft complaint, file online or mail it to DATCP:

- File a complaint online.
  - Fill out the form completely. An incomplete complaint form will make it difficult to investigate or refer your complaint. **Note:** You will need to have the Non-Consent Form notarized.
  - Upload copies of any documentation that supports your complaint.
- Download DATCP's Identity Theft Complaint Packet and mail your complaint, with supporting documentation, to DATCP at:
  - DATCP Bureau of Consumer Protection
    PO Box 8911
    Madison, WI 53708-8911

Or fill it in electronically and attach digital copies of your papers and e-mail to DATCPHotline@wisconsin.gov

Caution: Your complaint can be seen by others if they ask for it under Wisconsin's Open Records law. However, DATCP will keep your personal information private as much as the law allows. Before you send in your complaint, you can leave out or cover up private details (like your bank account number, credit card number, Social Security number, or birthday) if they aren't needed.

What happens to your complaint?

- Once they get your complaint, a Consumer Protection Investigator will evaluate the information to decide an appropriate course of action. The investigator will follow up with you within one week of receiving your complaint.
- Self-help information will be sent to you to help you get started on the path to recovering your identity.
- If DATCP believes an identity thief or business may have violated state laws, the Department may reach out to local law enforcement officials. If your complaint is part of a larger identity theft or identity fraud investigation, your complaint will be shared with the appropriate local, state, and federal authorities.

Report a Misused Social Security Number

If you suspect someone is using your Social Security Number for work purposes, contact the SSA to report the problem. SSA Fraud Hotline: 1-800-269-0271

Also ask about getting a Social Security statement that lists your annual earnings by year, along with potential Social Security monthly benefits at retirement. You can also get your Social Security statement online by creating an account at https://www.ssa.gov/myaccount/ and then using their online service to request a statement. If your earnings on this report do not match your actual earnings, that might mean someone is using your Social Security number to get employment. If you find errors, contact your local SSA office.

Replace Government-Issues IDs

Driver's License

Call your local service center of the Wisconsin Division of Motor Vehicles at (608) 264-7447 immediately to report the theft of your driver's license or state ID. The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a replacement license. To do this, you need to appear in person at your local DMV service center. Be sure to take with you proof of identity. Documentation showing your name and signature or name and picture will be considered acceptable proof of identity. You can also enroll in e-notification to receive email or text notifications when something occurs on your account: http://wisconsindmv.gov/enotify.

Passport

Call the State Department at 1-877-487-2778 or TTY 1-888-874-7793. If you want to replace the passport and you are traveling within the next two weeks, make an appointment to apply in person at a passport agency or center. If you are not traveling within two weeks, submit an Application for a Passport and Statement Regarding a Valid Lost or Stolen U.S. Passport in person at an authorized Passport Application Acceptance Facility.

Report Mail Fraud

Contact the U.S. Postal Service (USPS) if your mail is stolen or if someone has filed a change of address form fraudulently on your behalf at www.uspis.gov or (877)-876-2455.

Stop Debt Collectors from Collecting on Debt You Do Not Owe

- Write to the debt collector within 30 days of getting the collection letter. See this sample letter provided by the FTC.
    - Tell the debt collector someone stole your identity, and you don't owe the debt.
    - Send copies of your Identity Theft Report and any other documents that show the theft.
- Contact the business where the fraudulent account was opened
    - Explain that this is not your debt.
    - Tell them to stop reporting this debt to the credit bureaus.

    - Ask for information about the debt, and how it happened. The business must give you details if you ask. This sample letter can help.
        - For example, if someone opened a credit card in your name, ask for a copy of the application and the applicant's signature.
- If you have not already, ask the credit bureaus to block information about this debt from your credit report
    - See our article Disputing Errors on Credit Reports for more information.
- Write down who you contacted and when. Keep copies of any letters you send.

Report Tax-Related Identity Theft

To the Wisconsin Department of Revenue (DOR)

If someone uses your personal information to file a tax return, contact the DOR immediately by phone ((608) 266-2772)) or e-mail (DORIDTheft@wisconsin.gov). Complete the Identity Theft Declaration Form and mail it to:

Wisconsin Department of Revenue
Office of Criminal Investigation - ID Theft
PO Box 8906
Madison WI 53708-8906

To the Internal Revenue Service (IRS)

If you got a notice from the IRS that they rejected your return because someone already used your SSN or ITIN to file, immediately call the number on the notice.

Submit an Identity Theft Affidavit online or print out an Identity Theft Affidavit and submit it by mail or fax according to the instructions on the form.

If your problem still is not resolved, call the IRS at 800-908-4490.

Keep Records of Everything

Create a file with:

- Copies of letters and forms you send
- Names and phone numbers of people you speak to
- Copies of your police report and FTC report

- Notes of when you called and what was said

This documentation will help you resolve disputes and prove your case.

Consider an Identity Theft Protection Tool

Consider enrolling in:

- Credit monitoring services (some are free after fraud)
- Identity theft insurance, if you have it through your employer or financial institution

Summary Checklist

- Request credit reports and review them
- Contact affected companies
- File a police report
- File a report with FTC
- Place fraud alert or credit freeze
- File a report with DATCP
- Replace any stolen documents
- Contact debt collectors (if applicable)
- Notify WI DOR and IRS if tax-related
- Keep a record of all actions
- Consider ID-Theft Protection tools

Last updated on July 24, 2025.

Credit Reports Credit Cards & Reports

Print

Table of Contents

Our Partners