MICHIGAN ATTORNEY GENERAL

CONSUMER ALERT

IDENTITY THEFT PREVENTION (see also our Identity Theft Recovery Alert)

Identity theft happens when a thief steals your personal information without your knowledge to commit fraud or theft. Personal information is any information that can identify you and includes your: Social Security number, birthdate, address, passwords, account and credit card numbers, and anything used to answer security questions.

Knowing how to guard your personal information is your first line of defense against identity theft.

THINK LIKE AN IDENTITY THIEF

An identity thief needs your personal information to steal your identity. Where do you keep your personal information and who has access to it?

Identity thieves use low and high tech means to steal from you. They may dumpster dive or get into your hard drive through an online scam. They go where you have your personal information.

So even if you follow best practices for your cyber security and lockdown all of your online information, if you leave your front door unlocked or toss un-shredded documents containing your personal information in the trash, your personal information may be at risk.

Identity theft is often a silent crime. Experienced identity thieves may use your information for months—even years—while you remain unaware. You may not learn that you are a victim of identity theft until you are denied credit because of negative entries on your credit report. How can that happen?

You know when your wallet is stolen at a store or from your workplace, but you might not know about someone who works in your home who steals your information, or if mail is taken from your mailbox, or if a service person takes your information when you hand over your credit card.

You also will not know if an employee with access to your personal information is bribed to provide your personal information to criminals, or if it is gained in a security breach, or through an unsecure Wi-Fi connection, or from a hidden skimmer at an ATM machine or gas pump.

It is also quite possible that you unwittingly gave the identity thief your personal information when you answered a phishing phone call or email, or when you posted it on one of your social media accounts.

REDUCE YOUR RISK

At one extreme, reformed identity thief Frank Abagnale of “Catch Me If You Can” fame and current AARP Fraud Watch Network Ambassador, advises:

- charge everything to a credit card [you are most protected against liability for fraudulent charges];
- shred papers with a device that makes micro cuts [turns your documents into confetti];
- consider credit monitoring [know when someone checks your credit and more]; and
- never pay again with a personal check [you expose your account and routing number and hence, your money, to anyone who handles the check].

While that may be sage advice, it is not necessarily practical or optional for all. Here is a list of 20 things everyone can do:

1. Don't disclose personal information unless you know who you're giving it to, for what purpose, and how it will be protected.
2. Secure your Social Security card: don't carry it with you.
3. Carefully and promptly review statements for unauthorized charges or fraudulent use.
4. Shred all mail and other documents containing your personal information before discarding them.
5. Keep sensitive documents in a safe place at home.
6. Cancel all credit cards that you do not use.
7. Protect your mail: collect it promptly; place a hold on it while you are away; and don't use insecure mailboxes.
8. Stop receiving pre-approved credit offers in the mail by visiting optoutprescreen.com or by calling 888-5-OPTOUT (888-567-8688).
9. Other types of information-sharing that consumers may request businesses to block are listed on the World Privacy Forum's "Top Ten Opt-Out" web page.
10. Register with the Federal Trade Commission's (FTC) national do-not-call list to reduce telemarketing calls; online or by calling toll-free 888-382-1222.
11. Keep a secure master list or photocopies of important identification and account numbers, including the phone numbers of the customer service fraud departments of your card issuers.
12. Keep your passwords in a safe location. Don't record them on anything you carry with you. Never keep passwords or PINs near cards or documents identifying the account to which they belong.
13. Follow best practices online. Only connect to secure websites through secure internet connections; use two-factor authentication that requires the user to enter a one-time code each time they log into their account; update sharing and firewall settings; and consider using a virtual private network (VPN) if you use a public server or free Wi-Fi.
14. Create strong passwords. Experts recommend phrases or sentences with at least one randomly placed special character. (e.g., "Ireallllly%lovehamsandwiches")
15. Use and maintain anti-virus software and a firewall.
16. Enable security features on mobile devices — especially if you have contacts, banking websites and applications saved.
17. Do business with reputable companies—local and online. Verify secure websites and watch for phishing solicitations.
18. Check privacy policies. Know how a company will use or distribute your information: opt-out of allowing any company to share your information when you can.
19. Watch what you post on social media. Identity thieves are skilled at piecing together information from a variety of sources. Do not post personal information in public forums.
20. Order your free credit report from each of the three major credit-reporting agencies every year. Make sure it is accurate. Order one report from a different company every four months. You can order it free from annualcreditreport.com.

IDENTITY THEFT PREVENTION SERVICES

Companies may advertise that they provide identity theft prevention services, but no service can protect you from having your personal information stolen. What these companies can offer are monitoring and recovery services.

Monitoring services watch for signs that an identity thief may be using your personal information.

Recovery services help you deal with the effects of identity theft after it happens. (See the Attorney General's Consumer Alert, Identity Theft Recovery.)

Monitoring and recovery services are often sold together and may include options like regular access to your credit reports or credit scores.

CREDIT MONITORING SERVICES

Credit monitoring is a service that tracks your credit report and alerts you whenever a change is made. This gives you the opportunity to confirm the accuracy of the change and, if needed, contest any inaccuracy.

The specifics of any service depend on the provider; however, most notify you of any changes to your credit report within 24 hours.

The type of changes you can expect to receive alerts about include: hard inquiries, which are made when a credit card or loan application is submitted in your name; new accounts, which generate a note on your report whenever a new credit card or loan is opened in your name; changes to any existing accounts; and address changes.

Some companies extended their services to include non-credit red flags that monitor sex-offender registries, bank-account activity, or payday-loan applications. (See identity-monitoring services below.)

Credit monitoring companies may offer "free" trial periods followed by an expensive automatic renewal that can be difficult to cancel.

Credit monitoring only warns you about activity that shows up on your credit report — and many types of identity theft won't appear. For example, credit monitoring won't tell you if an identity thief withdraws money from your bank account or uses your Social Security number to file a tax return and collect your refund.

Some services only monitor your credit report at one of the Credit Reporting Agencies (CRAs). So, for example, if your service only monitors TransUnion, you won't be alerted to items that appear on your Equifax or Experian reports.

Prices for credit monitoring vary widely, so it pays to shop around.

Before you sign up for credit monitoring services, the Attorney General recommends you ask these questions to any provider you are considering:

- Which credit bureaus do you monitor?
- How often do you monitor reports? Some monitor daily; others are less frequent.
- What access will I have to my credit reports? Can I see my reports at all three credit bureaus? Is there a limit to how often I can see my reports? Will I be charged a separate fee each time I view a report?
- Are other services included, such as access to my credit score?

FRAUD-DETECTION OR IDENTITY-MONITORING PLANS

A fraud-detection or identity-monitoring plan goes beyond credit monitoring and fraud-alert services by checking other "public" records, such as criminal records, official filings regarding real estate transactions, employment records associated with your Social Security number, as well as some other places your information may appear, which could include chat rooms and national databases containing credit card applications.

Many of the steps included in fraud-detection plans can be taken by consumers without charge.

Further, fraud-detection services do not prevent ID theft and may not catch certain activity, such as medical ID theft and "fragmented" credit files (which are created when a thief combines your Social Security number with a different name and address to invent a new identity).

Before you sign up for fraud-detection services, the Federal Trade Commission recommends you ask these questions to any provider you are considering:

- What kinds of information do you check, and how often? For example, does the service check databases that show payday loan applications to see if someone is misusing my information to get a loan?
- What personal information do you need from me and how will you use my information?
- Are other services included with the identity-monitoring service? Do they cost extra?

ID THEFT INSURANCE

Identity theft insurance generally covers only out-of-pocket expenses directly associated with reclaiming your identity. Typically, these expenses are limited to things like postage, copying and notary costs. Less often, the expenses might include lost wages or legal fees. The insurance generally doesn't reimburse you for any stolen money or financial loss resulting from the theft.

Like any insurance policy, there may be a deductible, as well as limitations and exclusions. Also, most ID theft policies don't pay if your loss is otherwise covered by your homeowner's or renter's insurance. If you are interested in identity theft insurance, ask to see a copy of the company's terms and conditions.

As with any insurance policy, the Attorney General strongly urges consumers to read the fine print and especially look for unpublicized limitations, exclusions, and preconditions to filing claims.

CONTACT THE ATTORNEY GENERAL'S OFFICE

If you have a general consumer complaint, you may file a complaint with the Attorney General's Consumer Protection Unit:

Consumer Protection Unit
P.O. Box 30213
Lansing, MI 48909
517-335-7599
Fax: 517-241-3771
Toll free: 877-765-8388
Online complaint form

The Attorney General provides Consumer Alerts to inform the public of unfair, misleading, or deceptive business practices, and to provide information and guidance on other issues of concern. Consumer Alerts are not legal advice, legal authority, or a binding legal opinion from the Department of Attorney General.

MI.GOV/AGCONSUMERALERTS