IDENTITY THEFT PREVENTION

Consumer Alert

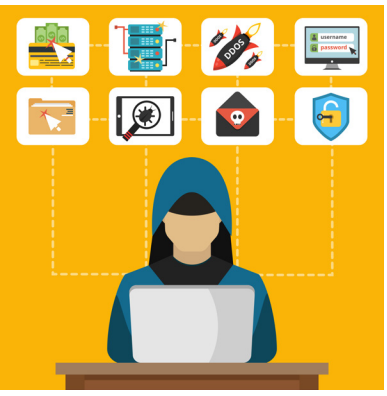
In the news:

Identity theft is the fastest growing crime in the U.S. On average, there is one identity theft victim in the U.S. every two seconds. And for Michigan consumers, the Federal Trade Commission reports that six of the top 15 cities for identity theft reports in 2016 were in Michigan—including the number one city: Ann Arbor.

What you need to know:

Knowing how to guard your personal information is your first line of defense against identity theft. This alert shares where identity thieves find your personal information and lists steps you can take to avoid becoming their victim.

Think like an identity thief



An identity thief needs your personal information—your name, social security number, credit card number, bank account and routing numbers, or login and password information to commit fraud and other criminal acts.

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 in to your hard drive thru 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 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 it 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 posted it on one of your social media accounts.

What you can do to reduce your risk

At one extreme, reformed identity thief Frank Abagnale, "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 microcuts [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].

Dana Nessel
Attorney General

IDENTITY THEFT PREVENTION

Consumer Alert

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 program to reduce telemarketing calls at the national registry online or by calling toll-free 888-382-1222.
11. Keep a secure master list or photocopies of all 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; update sharing and firewall settings; and consider using a virtual private network (VPN) if you use a public server or free-WiFi.
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

Consumer Alert

Identity theft prevention services

Many companies advertise their services as identity theft protection services. In fact, 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 will depend on the provider; however, most notify you within 24 hours of any change to your credit report.

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.

But 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 Agency (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 Federal Trade Commission recommends you ask these questions to any provider you are considering:

- Which credit reporting agencies do you monitor?
- How often do you monitor CRA reports?
- What access will I have to my credit reports?
- Can I see my reports at all three CRAs?
- 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?

IDENTITY THEFT PREVENTION

Consumer Alert

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.

According to Consumer Reports, these services range between $96 and $240 per year.

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?
- What personal information do you need from me and how will you use my information?
- Are other services included?
- Do they cost extra?

ID theft insurance

Offers for ID Theft insurance promising coverage for ID theft-related losses of up to $2,000,000 catch the attention of many consumers.

Before subscribing, consumers should ask and consider:

- What sort of losses the ID theft insurance policy covers and what exclusions apply;
- What is the cost of the policy and of any other services that must also be purchased;
- What protections are already being provided by banks and credit card companies against fraudulent charges, and are they adequate; and
- What are businesses who suffer security breaches potentially affecting your information likely to offer for no charge to their customers?

As with any insurance policy, the Attorney General strongly urges consumers to read the fine print. Insurance policies may contain unpublicized limitations, exclusions, and preconditions to filing claims.

For further information

Related Consumer Alerts from the Attorney General include:

- Identity Theft Recovery
- Credit Freeze; Fraud Alert; & Credit Monitoring
- Data Breaches: What To Do Next
- Don't Throw Away Your Right To Financial Privacy
- Equifax Breach
- Fraudulent E-mail Thieves Intend to Steal Your Personal Information
- Identity Theft: Deceased Victims
- Tax-Related ID Theft
- IRS Phone and Email Tax Scams

Inquiries and complaints may be directed to the Attorney General's Consumer Protection Division at:

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

Dana Nessel
Attorney General

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.