Consumer Tips on Identity Theft Prevention

Identity theft is the fastest growing crime in the country affecting thousands of consumers. By accessing and using basic information, a criminal can use your personal information to make unauthorized withdrawals of funds from your accounts, make fraudulent purchases with your credit cards, and create new accounts (banking, telephone, utility, loans, all of which can have a damaging effect on your credit).

The following are some tips to help you lower your risk of identity theft:

- Keep personal and financial records in a locked cabinet or in a password-protected file.
- Avoid providing your full 9-digit Social Security Number whenever possible. Always ask if you can provide the last four digits or use alternate information altogether.
- Do not carry your Social Security card.
- Enroll in direct deposit.
- Do not pre-print personal information (i.e. Social Security number and driver's license number) on your personal checks.
- Shred any documents that display personal and financial information before throwing in the trash.
- Be cautious with your mail. Incoming or outgoing mail should not sit in your mailbox for extended periods of time. Do not put checks in an unlocked mailbox.
- Never respond directly to requests for personal or account information online, over the phone, on email, or through a mobile device – including text messaging.
- If a request for personal or account information appears to come from your financial institution or credit card company, verify the request before providing any information. Contact your financial institution's official website or telephone number listed on your financial statements or on the back of your bank or credit cards.
- Be aware of the dangers of online threats. Install anti-virus and anti-malware software on your computer, and keep it updated. Install security patches and software updates as soon as they are released by verified sources.
- Use a separate credit card or account for on-line purchases.
- Don't publish your birthdate, email address, mother's maiden name, pet's name or other identifying or personal information on social networking sites.
- Use privacy settings on social networking sites to control who is able to access personal profile information.
- Use unique and hard-to-guess passwords that combine letters, numbers, and symbols.
- Change your passwords regularly. Use strong passwords for wireless Internet connections, and don't access unsecure Websites or type in personally-identifiable information using public Wi-Fi on mobile devices, laptops, or computers. Turn off Bluetooth and Wi-Fi when they are not being used.
- Review each of your three credit reports once a year to ensure all information is correct.

Don't be embarrassed or ashamed – fraud can happen to anyone at any age.

Resolving Identity Theft

If you suspect you are a victim of identity theft, you should take steps to report the crime and begin repairing your personal information. Resolving identity theft takes time, but taking action quickly is important to prevent the thief from doing more damage. Once you take immediate action, you should then monitor your progress as you work to correct your personal information.

The following are five steps to take immediately when identity theft strikes:

1. Contact all three credit reporting agencies to place fraud alerts. They can be contacted at www.annualcreditreport.com or by telephone at the following numbers:

   Equifax 800-525-6285
   Experian 888-397-3742
   TransUnion 800-680-7289

2. Close accounts that have been accessed and apply for new passwords.
3. File a complaint with the Michigan Attorney General 877-765-8388.
4. Call the Federal Trade Commission (FTC) Identity Theft hotline at 877-438-4338, or contact them online at www.ftc.gov. You will receive an ID Theft Affidavit.
5. File a police report and when you attach the ID theft affidavit this becomes an Identity Theft Report. This is necessary for providing persuasive evidence of theft in disputing debts.

It is important that you keep good written records of all of your activities and send all correspondence certified mail, return receipt requested, so you can document when correspondence is received. Creating a system to organize your calls and track deadlines will help you ensure corrections are made quickly. Once you have taken the initial steps, you should continue to monitor your personal information and ensure errors and problems are corrected.