

You're the *One*TM

PROTECT YOURSELF FROM IDENTITY THEFT

- Tear up or shred receipts, bank statements and unused credit card offers before throwing them away.
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help or are having work done in your house.
- Protect your PINs and passwords; use a 10-digit combination of letters and numbers for your passwords, and change them periodically. Avoid using easily available or guessed information like mother's maiden name, birth date, the last four digits of SSN or phone number, or a series of consecutive numbers.
- Monitor account activity on a regular basis. Sign up to view your financial accounts and billing statements online.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you've initiated the contact or are sure you know who you're dealing with.
- Do not carry your Social Security card.
- Give SSN only when absolutely necessary; ask to use other types of identifiers. Carry only identification information and credit/debit cards actually needed when going out.
- Report lost/stolen checks and cards immediately.
- Place an active duty alert on your credit report if deployed in the military.
- Personal computer safeguards:
 - Use and keep up-to-date firewall and anti-virus software protection.
 - Avoid using the auto-login feature.
 - Use strong passwords (alpha-numeric including special characters if possible).
 - Don't open emails or attachments from unknown sources.
 - Don't download files from strangers or click on hyperlinks from unknowns.
 - Keep current on security updates and patches.
 - Disconnect from the internet when not in use.
 - Use spyware/malware detection services
- Review your credit report to ensure accuracy. You may order free copies at annualcreditreport.com.

If You Become a Victim

- Contact one of the three major credit bureaus and request that a fraud alert be placed on your credit report:
 - Equifax, 800.525.6285;
 - Experian, 888.397.3742;
 - TransUnion, 800.680.7289.
- Close any accounts that may have been tampered with or opened fraudulently.
- Request that fraudulently opened accounts be blocked from reporting to the credit reporting agencies.
- File a report with your local police or the police in the community where the identity theft took place.
- Report the theft to the Federal Trade Commission at ftc.gov/idtheft or 877.438.4338.



MidWestOne.com
800.247.4418

