



RESOURCES FOR PROTECTING AGAINST CYBER FRAUD

Best Practices to prevent cyber fraud:

- Review your credit report annually by obtaining it for free from: www.annualcreditreport.com. Be sure to use this official site and not others with similar names that companies use to try to sell you services.
- Place a freeze on your credit reports at all three credit agencies:
 - Equifax: www.freeze.equifax.com
 - Experian: www.experian.com/freeze/center.html
 - TransUnion: freeze.transunion.com
- Monitor your existing credit card and bank accounts closely for charges or transactions you don't recognize. Notify the fraud departments of your bank and/or credit card company of any fraudulent activity on your accounts.
- Change your passwords on a regular basis and make sure they are "long and strong."
- File your taxes promptly — as soon as you have your tax information — to prevent tax identity theft. Respond right away to letters from the IRS, but never respond to phone calls or emails. Go to IRS.gov/taxscams/consumeralerts for more information.

If you become a victim of cyber fraud:

- Visit IdentityTheft.gov to file an online theft report with the FTC and to get an online recovery plan. Go to FTC.gov for additional consumer resources.
- Report Tax ID theft to the IRS: IRS.gov/identitytheft
- Report a lost or stolen Social Security number/card to: SocialSecurity.gov/myaccount
- Report Medical ID theft to: 1) your health insurance company, and 2) Medicare's fraud office at Medicarefraudcenter.org
- File a police report with your local authorities.