Protecting Your Identity

Basic rules:

- **Be careful to whom you give your information** (such as social security number, driver's license, computer passwords, etc). Protect yourself!
- **Don't trust phone calls, emails or texts from people you don't know.** Don't click on links.
- **Consistently check accounts.**

Social Security number: Do not carry your social security card in your wallet. Keep it in a safe place. Don't provide your social security number unless it is vital. Examples where it may be necessary: your work, your bank. Never give your full social security number over the phone or online. Most companies will just ask for the last four numbers.

Computer password: Don't leave your computer passwords in an easy-to-find location. Change computer passwords periodically. Make passwords strong, which means using capital letters, lower case letters, symbols and numbers. Vary passwords for different sites. You can even use password management software, but that probably isn't necessary if you create strong passwords and vary them periodically. Of course, if you think you may have been hacked, change your password immediately.

Banking and Credit Cards: Consistently check your bank account and credit cards for charges you haven't made. If you see anything suspicious, look into it immediately. If you did not make the charge, contact your bank (or credit card company) ASAP. You need to let them know you did not make the charge and ask them to cancel payment. You may need to cancel the credit or debit card and order a new one. Awareness is a key to protecting your identity.

Check your credit report: Get your free credit report annually. Sign up for Credit Carma or some other helpful credit reporting app. Check for any fraudulent activity and report it immediately. Do you see an account that you don't recognize? If so, contact one of the credit reporting agencies and create a fraud alert. (That credit reporting agency should contact the other two, but you could report the fraud to all three agencies.) That alert should last 90 days and can be extended if necessary.

Be aware of tricks hackers may use: You may have people send you an email or text that sounds like they know your password. Don't help them in any way. Don't respond. They are likely phishing for information. You may also get an email or text from someone that may seem

reliable, such as your bank. Don't click on links! Close the email or text and log into your bank or other account in the normal way. Consider contacting the bank or credit card company to check into the email.

Don't overshare on social media. Be restrained in what information you share. Are you heading out of town? Don't announce it. Avoid sharing your address or other contact info.

Don't provide a paper trail: shred or cut up any letters/material that provides credit card information or other personal info (such as a social security number). Shred/destroy credit card offers.

Signs of identity theft:

(information taken from https://www.amfam.com/resources/articles/money-matters/recover-from-identity-theft)

- If you see withdrawals from your bank account that you didn't make or can't explain.
- You have charges on your credit card that you didn't make.
- Debt collectors call you regarding debts that aren't yours.
- There are unfamiliar charges or accounts on your credit report.
- You get bills for utilities or medical services you didn't use.
- You aren't getting your bills or other mail.
- The IRS informs you that someone used your Social Security number for a tax refund or job.

If any of the above occurs, you need to address it immediately with the bank or credit card company or IRS or credit reporting agency. Don't ignore it!