- Watch your mailbox for stolen mail, which is one of the easiest ways for people to steal your identity.

Review Your Transactions & Statements:

- Order credit reports every year from each of the major credit reporting agencies and thoroughly review them for accuracy.
- Sign up for alerts from your bank, so you can track your transactions and quickly identify any that are suspicious.
- Check your monthly credit card and bank statements for unusual activity.

Practice Internet & Phone Safety:

- Be aware of *phishing* and *spoofing* – spam phone calls and emails from what seems to be a government entity or financial institution asking for sensitive information.
- If you are using a shared computer to check your bank balance or transfer funds, log-out of your account when you are finished to protect your money and information. Do not auto-save passwords.
- Do not download files sent to you by strangers or click on hyperlinks from people you don't know. Be aware of opening attachments in emails or text messages, as they could contain malicious software.
- Don't use public Wi-Fi for sensitive transactions, like banking or online shopping.
- Use a firewall program on your computer.
- Never give personal or financial information over the phone or Internet unless you initiated the contact. Be aware of common phone scams, which can be found here: https://www.consumer.ftc.gov/articles/phone-scams

Take Immediate Action:

- Freeze your credit with the three major credit bureaus if you suspect someone has stolen your information. This stops new lines of credit from being opened.
- Report lost or stolen credit or debit cards *immediately.*