Take steps to protect yourself from identity theft:

•Secure your Social Security number (SSN). Don’t carry your Social Security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary.

•Don’t respond to unsolicited requests for personal information (your name, birthdate, Social Security number, or bank account number) by phone, mail, or online.

•Contact the three credit reporting agencies to request a freeze of your credit reports.

•Collect mail promptly. Place a hold on your mail when you are away from home for several days.

•Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.

•Enable the security features on mobile devices, especially if you have contacts, banking websites and applications saved.

•Update sharing and firewall settings when you're on a public wi-fi network. Consider using a virtual private network, which can give you the privacy of secured private network.

•Review your credit card and bank account statements. Promptly compare receipts with account statements. Watch for unauthorized transactions.

•Shred receipts, credit offers, account statements, and expired credit cards, to prevent “dumpster divers” from getting your personal information.

•Store personal information in a safe place.

•Install firewalls and virus-detection software on your home computer.

•Create complex passwords that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases

•Review your credit report once a year to be certain that it doesn't include accounts that you have not opened.