Fraud Protection Checklist

In today's digital landscape, sophisticated identity theft and scams are on the rise. Here are some precautions you can take to safeguard yourself and your information.

#1 Educate yourself on common scams (and who they typically target.) Awareness is the first step in fraud prevention. Here are some frequently reported scams to watch out for:

Common Scams

Phishing: emails and texts that trick you into clicking on a link or opening an attachment (for example a request to update your current billing information.)

Tech support: receiving notice that your device is infected. Scammer will often offer to "fix" the problem in order to gain access to your account(s).

Prize/lottery scams: You're informed that you've won a prize or large sum of money and must submit a processing fee.

#2 Consider signing up with the National Do Not Call Registry to minimize telemarketing contact (it's free.)

#3 Protect your devices with anti-virus and spyware software. Routinely download any system updates (patches) to ensure your protection is up to date.

#4 Create strong, unique passwords for your online accounts. (Too many passwords to remember? Most smartphones provide the option to store passwords, or you can also download a trusted password manager app.)

#5 Avoid emails or texts that request details such as your credit card number, account number, social security number or password. Many scammers pose as financial employees, government officials or law enforcement. If you wish to verify their identity, visit their company website directly (or confirm contact details listed on statements or official correspondence.)

#6 Set up credit monitoring to track your credit score, monitor your spending, and receive immediate alerts for any suspicious activity on your account. Your financial institution may offer this for free.

#7 Never send money to anyone outside of your trusted contacts, and thoroughly verify the request is legitimate before sending funds.

#8 Vet caregivers, household managers or personal assistants that may have access to your information. Hire through a bonded agency that utilizes a rigorous screening process.

#9 If you have been a victim of an online scam, contact your financial institution immediately and file a complaint with the Federal Trade Commission. (Mail scams can be reported to the U.S. Postal Inspection Service.)

#10 Communicate regularly with any family members involved in your finances and connect with GreenPath for a credit report review that can help alert you to any fraudulent activity.