Identity Theft Protection Checklist

Freeze Credit and Establish Online ID with Government

#1 Freeze/Lock Your Credit Report with All Three Nationwide Credit Bureaus

1) **Experian**: www.experian.com/freeze/center.html or call 888-397-3742
2) **TransUnion**: www.transunion.com/credit-freeze or call 888-909-8872
3) **Equifax**: www.equifax.com/personal/credit-report-services/ or call 800-349-9960

#2 Establish your identity at ID.ME

1) Go to www.id.me, then choose Internal Revenue Service; "Connect with ID.ME"
2) **Set an IRS Identity Protection (IP) PIN**: Use the ID.me account to sign into www.irs.gov, or go directly to: www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
3) Establish control of your **Social Security Administration account**: https://ssa.gov and follow prompts to login to "my Social Security" using ID.me.

#3 Monitor your credit reports and all online accounts (Take note of all changes)

1) Annually: Get credit report from AnnualCreditReport.com - Do now if not done recently!
2) Ongoing: Take note of all changes to account information: email, financial, shopping, Google, Microsoft, Apple, social media, etc.

Purchase ID Theft Insurance

It is strongly recommended to purchase **ID Theft Insurance**. A basic plan like: Zander, Allstate [Basic], McAfee, Complete ID, etc. should be enough. Compare "Basic" vs. "Premier" & individual vs. family options. Start research here: www.safehome.org/compare/identity-theft-protection/

If you have **diligently done *everything* else on this page**, then you may decide to take on extra risk and save money by not purchasing ID Theft Insurance. If so, you must take extra care to regularly monitor all your accounts and credit reports.

Implement Strong Digital Defenses

#1 Use a Password Manager program (w/strong, unique password for each account)

#2 Set up 2-factor/multi-factor authentication for all important accounts.
(Authenticator App if possible; SMS/Text if that is all you can do or only option available)

- Bank and other Financial and all Shopping accounts; including all accounts created above!
- Email and Google, Microsoft, Apple, etc. // All social media accounts
- Home related: Utilities, Phone, etc.

#3 Apply security updates/patches regularly/monthly (Computer, Smartphone, Apps, etc.)

#4 Avoid falling victim to social engineering scams (Take time to educate yourself on scams! Be aware of emails, texts, phone calls, etc. that you did not initiate. Don't click links. Never give out verification code to anyone!)

#5 Turn on Account Alerts (Change Notifications) for all important accounts: Email, financial, shopping, Google, Microsoft, Apple, social media, etc.

#6 Other Cybersecurity Hygiene: Antivirus, Full Disk Encryption, VPN, Backup data, minimize browser plug-ins, etc.

For more details about each of these items and more, please see: www.ComputerSecurityNW.com

Version 1.2, by Corey K., Jan.2023