Identity Theft and Cybersecurity Checklist

Safeguard as much as you can

These basic steps help you know what's on your credit files, lock them down and spot problems.

1. Get up to speed on your credit reports:

- ☐ You get a free copy from the credit bureaus every 12 months, via AnnualCreditReport.com.
- ☐ Supplement that by signing up for a free credit score and report that you can check whenever you like. NerdWallet offers both.

2. Secure your credit files. Your choices:

- ☐ Credit freeze — the best protection but it may carry fees; you have to lift the freeze when you want to apply for credit.
- ☐ Credit lock and credit monitoring — less of a hassle to lift; may carry a monthly fee, which adds up.
- ☐ Fraud alert — free, but lower protection; generally have to be renewed after 90 days unless you're active military or an ID theft victim.

3. Watch your accounts:

- ☐ Monitor credit card and bank statements for activity you don't recognize.
- ☐ Set up text alerts so you know when charges are made on your cards.
- ☐ Watch your free credit score and credit report for activity you can't explain.

Respond when put at risk

If you suspect personal information was exposed in a data breach or used fraudulently, take further steps depending on the type of information it was:

SOCIAL SECURITY NUMBER

Secure your account:

- [ ] Set up your mySocialSecurity account if you haven't already.

Check for damage:

- [ ] Review your work history at mySocialSecurity and report errors.
- [ ] Review your credit reports for fraudulent accounts.
- [ ] If you see fraudulent activity, create an identity theft report with the Federal Trade Commission, then use it to file a report with your local police.
- [ ] Save the FTC and police report numbers to use in repairing damage.

Repair the damage:

- [ ] Close fraudulent accounts.
- [ ] Use the credit bureaus' dispute process to remove fraudulent accounts and charges from your reports.

Remain on guard:

- [ ] File your taxes as early as possible to get ahead of any scammers attempting to hijack your refund.
- [ ] Pay attention to signs someone has gotten medical benefits using your information.

DEBIT OR CREDIT CARD NUMBER

- [ ] Ask the bank or card issuer to cancel the card; act quickly to limit your liability.
- [ ] Report any misuse; dispute fraudulent charges to get them off your credit reports.
- [ ] Remember to change any automatic payments that were on the old card.

A PASSWORD OR LOGIN INFORMATION

- [ ] Change your password; ask the company if you can change your username.
- [ ] If you can't log in, contact the company about shutting down the account.
- [ ] Change the password on any other site where you used the same password.
- [ ] If the site held your financial or credit card info, watch for fraudulent charges.

FINANCIAL ACCOUNT INFORMATION

- [ ] Contact the bank, credit union or other financial institution to close the account and open a new one.
- [ ] Watch your accounts carefully; if you see suspicious activity, alert the institution's fraud department.
- [ ] Remember to update any automatic payments that used the old account.

Sources: NerdWallet, Federal Trade Commission