9800 Fredericksburg Road
San Antonio, Texas 78288

Identity Theft Resolution Guide

Starting your identity theft recovery process consists of taking critical steps as soon as possible. Knowing what to do first and whom to contact are crucial. USAA is here to help you with the key steps:

1. **Obtain, review, and monitor your credit reports.** Request a free copy of your credit report by visiting AnnualCreditReport.com or by calling 877-322-8228. After you receive your credit reports, review them thoroughly.
   - Verify that all your personal information is correct, including your name, address and Social Security number.
   - Review, identify, and dispute unauthorized inquiries and accounts.

2. **Complete and print an Identity Theft Report.** This form is available at identitytheft.gov or call the Federal Trade Commission at 877-438-4338. An Identity Theft Report can help you dispute unauthorized accounts.

3. **Contact the three major credit bureaus.** Ask to have a fraud alert placed on your credit file. The following alert types may be placed:
   - **Initial Alert.** This alert will be placed in your file for one year. The alert will notify potential creditors or lenders that you are a victim of identity theft. You will only need to place a fraud alert with one credit bureau; the other two credit bureaus will automatically be notified.
   - **Extended Alert.** If you are a victim of identity theft, you can send the credit bureau an identity theft report and request that an extended alert be placed on your file. The extended alert remains in place for seven years and requires creditors to verify your request by contacting you at the phone number or numbers that you provided to the credit bureau.
   - **Active Duty Alert.** If you are on active military duty, you can add an active duty alert to your file. This is similar to the other alerts but remains in place for 12 months.
   - **Security Freeze.** A security freeze will allow you to restrict creditors from approving credit, loans and services in your name without your consent. You will be provided an identification number or password to use to temporarily release access to your credit report.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

4. **Notify the Internal Revenue Service (IRS).** If you know or suspect your Social Security number has been compromised or used to fraudulently file tax returns, complete IRS Form 14039 at irs.gov or by calling 800-908-4490.

5. **Protect all your accounts.** Review your personal profile and accounts with your financial institutions to identify any unauthorized activity. Protect all your financial, wireless, internet, and email accounts by using the strongest security options available.

6. **Establish a strong defense using the recommendations below.**
   - Enable multifactor authentication (MFA) as an extra layer of protection for your accounts to help reduce the risk of fraud. Learn more at usaa.com/mfa.
   - Review and respond to security and fraud alerts. USAA may notify you when changes are made to your personal information or security settings, or if we detect suspicious financial activity.

- Watch out for malicious software and phishing emails.
  - USAA corporate emails display the USAA Security Zone stamp in the upper right corner of the email to help identify emails sent from USAA.
  - **If you are suspicious about emails or websites claiming to be from USAA, please notify us immediately at abuse@usaa.com.**
- Limit your risk of installing malicious software by only downloading trusted applications from an application marketplace or store.
- Don't open files, click on links or download programs sent by unknown entities or persons. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.
- Keep antivirus software and operating systems up-to-date to prevent hackers from taking advantage of security flaws. Antivirus software scans your computer for viruses, spyware, and incoming email to block malicious files.