VWG WEALTH MANAGEMENT
A Hightower Company

Identity Theft Victim

Steps to Help Protect Yourself (2026)

What to do if your Social Security number or other personal information has been stolen or compromised:

- [ ] 1. Visit IdentityTheft.gov to report identity theft and get a recovery plan. This FTC-managed website walks you through each step of the recovery process and provides customized recovery guidance. Federal Trade Commission Hotline: (877) 438-4338. Website: https://www.identitytheft.gov
- [ ] 2. If your Social Security number has been stolen, contact the Internal Revenue Service (IRS). Identity thieves may use your SSN to file fraudulent tax returns, claim refunds, or obtain employment using your identity. IRS Identity Theft assistance is available at (800) 908-4490. In addition, obtain an Identity Protection PIN (IP PIN) to help prevent fraudulent tax filings. Website: https://www.irs.gov/identity-theft-central
- [ ] 3. File an online complaint with the Internet Crime Complaint Center (IC3). The IC3 provides a centralized reporting mechanism for cybercrime victims and forwards complaints to appropriate law-enforcement or regulatory agencies. Website: https://www.ic3.gov
- [ ] 4. Freeze your credit. A security freeze helps prevent criminals from opening new credit accounts in your name. Credit freezes remain free under federal law. Contact all three major credit bureaus: Equifax (800-349-9960), Experian (888-397-3742), and TransUnion (888-909-8872) or use their online security-freeze portals.
- [ ] 5. Monitor your credit reports regularly. Even after freezing your credit, review reports for unauthorized accounts, inquiries, or transactions. Obtain free credit reports through AnnualCreditReport.com and review all information carefully.
- [ ] 6. Notify your financial advisor, CPA, banks, credit unions, brokerage firms, retirement custodians, insurance providers, and other financial institutions. Request account monitoring, fraud alerts, and additional authentication measures where available.
- [ ] 7. Set up credit monitoring and fraud alerts. Services such as Credit Karma and monitoring tools offered by financial institutions can help identify suspicious activity quickly.
- [ ] 8. Review all financial accounts, including bank accounts, credit cards, investment accounts, retirement plans, digital payment accounts, and insurance accounts. Investigate any unfamiliar transaction immediately.

- [ ] 9. Change passwords on email, banking, social media, cloud storage, and financial accounts. Enable multi-factor authentication (MFA) wherever available and consider using a password manager to create and store unique passwords.
- [ ] 10. Protect against tax-related identity theft by creating and maintaining an IRS Identity Protection PIN (IP PIN). The IP PIN is a six-digit number known only to you and the IRS and significantly reduces the risk of fraudulent tax-return filings.

2026 Enhancements and Best Practices

- [ ] Use multi-factor authentication on all critical accounts.
- [ ] Monitor data-breach notifications and change credentials immediately if exposed.
- [ ] Keep operating systems, browsers, and mobile devices updated.
- [ ] Be cautious of phishing emails, texts, and telephone scams requesting personal information.
- [ ] Maintain documentation of all reports, correspondence, and case numbers related to the identity-theft incident.