

What You Can Do to Protect Yourself

Because your personal information has been compromised

1. **Enroll in a credit monitoring** service that will help you monitor your accounts for unexpected credit activity. Numerous services are available at no cost.
2. **We suggest you follow the identity protection process outlined by the FTC** (www.consumer.gov/idtheft). This process includes the placement of a "Fraud Alert" on your personal credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. To place a fraud alert on your file, you should call any one of the three major credit bureaus listed below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

Equifax
800-525-6285

Experian
888-397-3742

TransUnion
800-680-7289

3. Call the IRS fraud reporting office at 800-908-4490 to report compromised tax information.
4. After calling the IRS, fill out the individual IRS forms 14039. The form is available here: <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. Also contact your state tax authority separately because the IRS cannot disclose tax information to the state.
5. Determine what other precautionary measures might be appropriate for your circumstances.
 - a. **Consider obtaining an IRS Electronic PIN**, if you do not already have one. Visit <http://www.irs.gov/Individuals/Electronic-Filing-PIN-Request> or call 866-704-7388 and follow the systems prompts.
 - b. **Manage Personal Information:** Take precautionary steps to protect personal information, such as carrying only essential documents. Be aware when sharing information.
 - c. **Use Tools from credit providers:** Carefully review credit reports, bank, credit-card, and other account statements at least quarterly. Proactively create alerts on credit cards and bank accounts for suspicious activity. If unauthorized or suspicious activity is discovered, do not delay. Take action immediately.