HBK CPAs & Consultants

Identity Theft – What Can I Do?

The Federal Trade Commission estimates that more than 9 million Americans will have their identity stolen this year.

James M. Rosa, CPA, PFS
Chairman, HBK Tax Group
Principal, HBK CPAs & Consultants

Jim Rosa is Chairman of the HBK Tax Group and a Principal in the Tax Department in the Youngstown, Ohio office of HBK CPAs & Consultants. He has been with the firm since 1986.

Jim has extensive experience in personal and estate planning, charitable planning, tax-exempt organizations, and individual tax and financial planning. He also has experience in tax policies, procedures and resources, which HBK uses in their tax practices. Jim provides counsel to high-net worth individuals throughout HBK. He is one of the firm's preeminent presenters and specializes in addressing on topics such as the Affordable Care Act, shale energy planning, charitable giving opportunities, estate and gift planning, and exempt organization issues.

Jim earned a Bachelor of Science degree in Business Administration from the University of Toledo. He holds the Personal Financial Specialist (PFS) designation, which is awarded by the American Institute of Certified Public Accountants to recognize CPAs who provide financial planning service.

While the IRS has implemented return processing filters to make it more difficult for thieves to steal identities and file fraudulent returns, there are many ways in which you can limit your exposure to identity theft. At HBK CPAs & Consultants, we take these matters seriously and would like to provide you with information on ways to protect yourself.

Limit the flow of your personal information.

Personal information typically includes a person's marital status, birthdate, social security number, mother's maiden name, birthplace, etc. You can protect this information by shredding and destroying any personal or financial documents, keeping your social security card in a safe and secure location, and limiting the amount and type of information that you publish to social media. In addition, you should ensure that you have reputable security software installed and properly updated on your computers and other devices, and that any wireless networks you have are secured with a password. Avoid entering usernames and passwords while using a shared internet connection or a public wireless network, as these connections are vulnerable.

Check your information on a regular basis.

In addition to continuously checking credit card and bank statements to make sure there is no unauthorized use, it is also a good idea to monitor your credit report on a regular basis. Each of the three credit reporting agencies are required to provide you with a free report at least once per year. To obtain your free reports, visit www.annualcreditreport.com. In addition, it's a good idea to review your work history with the U.S. Social Security Administration. This can also be done online by creating an account at www.socialsecurity.gov/myaccount.

Know what to do if your identity has been stolen.

In the unfortunate event that your identity is stolen, there are a number of steps that should be taken right away in order to put a stop to the theft:

1. Call the company or institution where you discovered the fraud and notify them of the theft. Request that it close or freeze your accounts, and then change any login, password or PIN information you may have.
2. Place a fraud alert on your credit report by contacting one of the three credit reporting companies. The company will then notify the other two companies of the fraud alert. You should then request a free copy of your credit report and review it for any accounts or transactions you don't recognize.
3. Contact the Federal Trade Commission to notify them that your identity was stolen. This can be done online at www.identitytheft.gov. The FTC website will also walk you through these steps and help you create a recovery plan.

Once the theft has been reported and your accounts are secure, you will need to start mitigating the damage that was done. Any fraudulent accounts that were opened should be closed, fraudulent charges should be removed from your accounts, and your credit report should be corrected. You should consider taking advantage of an identity theft monitoring agency, and should place an extended fraud alert or credit freeze on your account.

Take these additional steps if you are a victim of tax-related identity theft.

Many of our clients find out that their identity has been stolen because they receive an IRS notice with inaccurate information, or they are unable to file a return electronically because one has already been filed under their social security number. In either these events, the following steps should be taken immediately:

1. Respond to any IRS notices right away by either calling the IRS at the number provided on the notice, or contacting us at HBK. If the notice instructs you to verify your identification, you should visit www.idverify.irs.gov and follow the steps provided. You will need to have the following information available:
    - Your prior year tax return;
    - Your current year tax return, if filed;
    - Any supporting documents, such as W-2s or 1099s.
2. If your e-filed return was rejected because of a duplicate filing, complete Form 14039, Identity Theft Affidavit, and mail or fax it to the IRS along with proof of your identity.
3. Continue to file your tax return and pay all taxes owed, even if you have to paper file.

Learn more about the Identity Protection PIN Program.

If you are a victim of tax-related identity theft and follow the above steps, the IRS will automatically issue you an Identity Protection (IP) PIN. The IRS may also issue you an IP PIN if it identifies you as a victim of identity theft, or if you are a resident of Florida, Georgia, or the District of Columbia and you participated in the IP PIN pilot program.

The IP PIN is a six-digit number that the IRS assigns to eligible taxpayers to help prevent the misuse of their social security number on fraudulent federal income tax returns. The IP PIN helps the IRS verify a taxpayer's identity and accept their electronic or paper tax return.☐