Identity Theft Information for Tax Professionals

Cross References

- FS-2017-04, March 2017

Tax professionals play a critical role in assisting clients, both individuals and businesses, who are victims of tax-related identity theft. The IRS, state tax agencies and the tax industry are working to prevent and detect identity theft as well as reduce the time it takes to resolve these cases.

What is tax-related identity theft? Tax-related identity theft occurs when someone uses a Social Security Number (SSN) (either a client's, a spouse's, or dependent's) to file a tax return claiming a fraudulent refund. Thieves may also use a stolen Employer Identification Number (EIN) from a business client to create false Forms W-2 to support refund fraud schemes.

How to know if a client is a victim of tax-related identity theft. Tax professionals may be unaware a client is a victim of identity theft until they attempt to file the tax return and it is rejected as a duplicate return. Other indicators include receiving a notice regarding:

- More than one tax return filed using the client's SSN.
- A balance due, refund offset or collection action taken for a year in which no return was filed.
- IRS or state records indicate the client received wages from an unknown employer.
- An amended tax return, fictitious employees or about a defunct, closed or dormant business (for business clients).

Did someone file a tax return or Form W-2 using a client's SSN? If a client's SSN has been compromised, whether from a data breach, computer hack or stolen wallet, and they have reason to believe they are at risk for tax-related identity theft, tax pros should take these steps:

- If the client received an IRS or state notice, respond immediately.
- Complete IRS Form 14039, *Identity Theft Affidavit,* if directed to do so by the IRS or if the client's e-file return rejects because of a duplicate SSN and there are no other errors (example: transposed numbers). Fax or mail to the IRS according to the instructions.
- Follow identity theft reporting procedures provided on the client's state revenue agency website.
- To inquire about specific client return information, preparers must have a power of attorney on file and must authenticate their identity with the IRS or state customer service representative.

What can preparers do if a client is a victim of identity theft? The Federal Trade Commission, the lead federal agency on general identity theft issues, has recommended steps identity theft victims should take to protect their credit. See www.identitytheft.gov for general recommendations for clients. Other steps include:

- For identity theft victims who previously contacted IRS and have not achieved a resolution, contact IRS for specialized assistance at 800-908-4490. Contact state revenue agencies per the website's instructions.
- Clients should continue to file returns and pay taxes, even if it must be done by paper.

How can preparers protect clients' sensitive information?

- When providing clients with copies of their tax returns, preparers can redact or mark out the Social Security Numbers and bank account information for client protection.
- The IRS, state tax agencies and the tax industry have launched an ongoing awareness campaign for taxpayers. See https://www.irs.gov/individuals/taxes-security-together for details. A similar awareness effort is directed at tax professionals. See https://www.irs.gov/individuals/protect-your-clients-protect-yourself for details.
- Be aware that tax preparation businesses can become a target for criminals. Follow IRS security guidelines in Publication 4557, *Safeguarding Taxpayer Data,* for protecting taxpayer information.