THETAXBOOK News Release Date: 11/23/15

# Identity Theft

## Cross References

- www.irs.gov
- IRS Pub 4557, *Safeguarding Taxpayer Data*
- IRS Pub 5027, *Identity Theft Information for Taxpayers*
- IRS Pub 5199, *Tax Preparer Guide to Identity Theft*

At a recent tax seminar attended by authors from *TheTaxBook,* the speaker said certain IRS administration officials with knowledge of the subject told him unofficially that 7% of electronically filed tax returns this past filing season were fraudulent, and that due to budget cuts, only seven IRS employees were available to work on resolving these identity theft cases. The IRS is aware that requiring PINs or electronic passwords could prevent most cases of identity thieves from filing fraudulent returns, but their computer systems are too old and outdated to handle all of the PINs that would be required for every taxpayer in the nation to use one.

Tax-related identity theft occurs when someone uses a taxpayer's stolen Social Security number and name to file a tax return claiming a fraudulent refund. Often, the taxpayer does not know his or her name and Social Security number has been stolen until he or she tries to file a legitimate tax return. The electronically filed return then gets rejected with an error code stating the taxpayer has already filed a return using that name and Social Security number. The legitimate taxpayer then has to go through a long process with the IRS in trying to resolve the issue, leading to delays in any legitimate refunds due the taxpayer.

This article discusses the steps to take when a taxpayer's identity has been stolen, along with helpful suggestions on avoiding identity theft.

## Steps to Take When a Taxpayer Becomes a Victim of Identity Theft

- File a police report.
- File an FTC complaint at www.ftc.gov and learn how to respond to it at identitytheft.gov.
- Contact one of the three major credit bureaus to place a fraud alert on the taxpayer's credit records:
  - Equifax, www.Equifax.com, 1-800-525-6285
  - Experian, www.Experian.com, 1-888-397-3742
  - TransUnion, www.TransUnion.com, 1-800-680-7289
- Contact the taxpayer's financial institutions and close any accounts opened without the taxpayer's permission, or accounts that have been tampered with.

It the taxpayer's Social Security number is compromised and the taxpayer knows or suspects he or she is a victim of tax-related identity theft, take these additional steps:

- Respond immediately to any IRS notice and call the number provided.
- Complete IRS Form 14039, Identity Theft Affidavit. Use a fillable form at www.irs.gov, print, then mail or fax according to the instructions on the form.

- Continue to pay taxes and file tax returns, even if paying and filing returns must be done by paper filing.

If the taxpayer previously contacted the IRS and did not have a resolution, contact the Identity Protection Specialized Unit at 1-800-908-4490.

## How to Reduce Risk of Identity Theft

- Don't routinely carry a Social Security card or any document with the taxpayer's SSN on it.
- Don't give a business the taxpayer's Social Security number simply because they ask. Only provide a SSN when absolutely necessary.
- Protect personal financial information at home and on the taxpayer's computer.
- Check the taxpayer's credit report annually.
- Check the taxpayer's Social Security Administration earnings statement annually.
- Protect personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts.
- Don't give personal information over the phone, through the mail, or the Internet, unless the taxpayer initiated the contact or is sure he or she knows who is asking for the information.

**IRS contact.** The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Report suspicious online or emailed phishing scams to:
phishing@irs.gov, or 1-800-366-4484.
Report IRS impersonation scams to the Treasury Inspector General for Tax Administration.

## Data Breach

A data breach is the intentional or unintentional release or theft of secure information. It can be the improper disposal of personally identifiable information in the trash or a sophisticated cyber-attack on corporate computers by criminals. It can affect companies large or small.

Not every data breach results in identity theft, and not every identity theft is tax-related identity theft. A taxpayer's tax account is most at risk if the data breach involves both a Social Security number and financial data, such as wages. Data breaches involving just credit card numbers, health records without SSNs or even drivers' license numbers, while serious, will not affect the taxpayer's tax account. The IRS stops the vast majority of fraudulent tax returns. If fraud is suspected, the IRS will contact the taxpayer via mail (not email) with instructions.

## Steps to Take When Taxpayer is a Data Breach Victim

1) If possible, determine what type of Personally Identifiable Information (PII) has been lost or stolen. It is important to know what kind of information has been stolen so the appropriate steps can be taken. For example, a stolen credit card number will not affect the taxpayer's IRS tax account.

2) Stay informed about the steps being taken by the company that lost the data. Some may offer special services, such as credit monitoring services, to assist victims.
3) Follow the Federal Trade Commission recommended steps, including:
   - Notify one of the three major credit bureaus (listed above) to place a free fraud alert on the taxpayer's credit file,
   - Consider a credit freeze, which will prevent access to the taxpayer's credit records,
   - Close any accounts opened without the taxpayer's permission,
   - Visit www.identitytheft.gov for additional guidance.
4) If the taxpayer received IRS correspondence indicating he or she may be a victim of tax-related identity theft or the e-file tax return was rejected as a duplicate, take these additional steps with the IRS:
   - Submit an IRS Form 14039, *Identity Theft Affidavit.*
   - Continue to file tax returns, even if it must be done by paper, and attach the Form 14039.
   - Watch for any follow-up correspondence from the IRS and respond quickly.

Form 14039 should only be used if the taxpayer's Social Security number has been compromised.

## Requesting a Copy of the Fraudulent Return

A victim of identity theft or a person authorized to obtain the identity theft victim's tax information may request a redacted copy (one with some information blacked-out) of a fraudulent return that was filed and accepted by the IRS using the identity theft victim's name and SSN. Due to federal privacy laws, the victim's name and SSN must be listed as either the primary or secondary taxpayer on the fraudulent return, otherwise the IRS cannot disclose the return information. For this reason, the IRS cannot disclose return information to any person listed only as a dependent.

Partial or full redaction will protect additional possible victims on the return. However, there will be enough data for the taxpayer to determine how his or her personal information was used.

To make the request, prepare a signed letter with the information described below and mail it and any additional documentation to the following address:

IRS
P.O. Box 9039
Andover, MA 01810-0939

The IRS may return a request if it is missing the required information and/or documentation, or is made in a manner other than described in these instructions.

**Required information and documentation for a request by the identity theft victim.** If the taxpayer is the person whose name and SSN was used to file a fraudulent tax return, the letter must contain the following information:

- Taxpayer's name and SSN.
- Taxpayer's mailing address.
- Tax year(s) of the fraudulent return(s) the taxpayer is requesting.

- The following statement, with the taxpayer's signature beneath: "I declare that I am the taxpayer."

A letter must be accompanied by a copy of the taxpayer's government-issued identification (for example, a driver's license or passport).

**Required information and documentation for a request by a person authorized to obtain the identity theft victim's tax information.** A letter submitted by a person authorized to obtain the identity theft victim's tax information must contain the following information:

- Name and tax identification number (such as a SSN) of the person authorized to obtain the information.
- The authorized person's relationship to the victim of identity theft (for example, parent, legal guardian, or authorized representative).
- Mailing address of the authorized person.
- Centralized authorization file (CAF) number if the authorized person was assigned one by the IRS for an authorization that is on file with the IRS covering the requested tax year(s).
- Tax year(s) of the fraudulent return(s) being requested.
- The taxpayer's name and SSN.
- The taxpayer's mailing address.
- The following statement, with the authorized person's signature beneath: "I declare that I am a person authorized to obtain the tax information requested."

The letter must be accompanied by a copy of the authorized person's government-issued identification (for example, a driver's license or passport). Also include documents demonstrating that person's authority to receive the requested tax return information (for example, Form 2848, Form 8821, or a court order) unless:

- The authorized person is requesting return information of his or her minor child as a parent or legal guardian, or
- The authorized person's authority to obtain return information for the requested tax year(s) is on file with the IRS and the authorized person is providing his or her CAF number.

## Business Identity Theft

Business identity theft happens when someone creates, uses, or attempts to use the identifying information of a business without authority to obtain tax benefits. Business identity thieves file fraudulent business returns to receive refundable business credits or to perpetuate individual identity theft.

Business identity theft is more complex than individual identity theft. Many of the same indicators that signify simple filing or processing errors also hint at business identity theft. While on the surface these occurrences may appear to indicate business identity theft, they may also stem from something as simple as transposed numbers.

- A taxpayer receives IRS notices about fictitious employees.
- A taxpayer notices activity related to or receives IRS notices regarding a defunct, closed or dormant business after all account balances have been paid.

- A taxpayer's return is accepted as an amended return, but the taxpayer has not filed a return for that year.

If any of the above occurs, the taxpayer will need to do some research before determining the incident is a result of identity theft.

Taxpayers may be victims of identity theft not related to tax administration if they:
- Receive bills for business lines of credit or credit cards they do not have.
- Notice that a credit report indicates credit or other open accounts they did not authorize.
- See unexplained bank account withdrawals.
- Don't get their bills or other mail.
- Find unfamiliar accounts or charges on their credit report.
- Get a notice that information was compromised by a data breach at a company where they do business or have an account.

If a taxpayer is a victim of identity theft not related to tax administration, file a report with the Federal Trade Commission at www.ftc.gov.