BDO

Wolters Kluwer CCH

CCH Tax Briefing

Identity Theft Update

October 8, 2015

Special Report

HIGHLIGHTS

- Identity Theft Incidents on the Rise
- Federal Identity Theft Statutes Pass
- State Identity Theft Statutes Pass
- IRS Takes New Measures to Combat Identity Theft
- Best Practices for Protecting Personally Identifiable Information
- Top Indicators/Responses to Tax-Related Identity Theft

INSIDE

As Identity Theft Grows, IRS and Practitioners React

The volume and magnitude of identity theft incidents have grown to an alarming extent. Last year, more than 9.9 million Americans were victims of identity theft, a crime that cost them roughly $5 billion. Tax-related identity theft crimes have also risen dramatically. TIGTA reports that 2,416,773 taxpayers were affected by identity theft in 2013, nearly double the number of victims in 2012, nearly quadruple the number in 2011, and nearly ten times the number in 2010. Predictions say the number of victims will again show an increase when 2014 and 2015 tax-year return statistics come in, even though the IRS and practitioners have been reacting more aggressively to stem the tide.

Tax-related identity theft most commonly occurs when an individual uses another taxpayer's Social Security number (SSN) to commit:

(1) "refund-related" identity theft, by filing a false tax return and obtaining a fraudulent refund; or
(2) "employment-related" identity theft, by obtaining a job, and leaving the unpaid income tax bill on the victim's account.

Identity Theft–Statutory Reaction

Identity theft is a particular kind of fraudulent misrepresentation, involving the unauthorized use of another's personal identification information that is most often accompanied by larceny. Until recently, the judicial focus was on the fraud committed, and was unaffected by whether or not a person's identification information had been utilized in the fraud. It was not until the very end of the 20th Century that federal and state governments enacted laws to levy separate and additional penalties for fraud committed using stolen identity information. In many instances, the commission of fraud is no longer required, as states have criminalized the unauthorized possession, purchase, sale, or distribution of personally identifiable information.

Federal Identity Theft Statutes

In 1998, Congress passed the Identity Theft and Assumption Deterrence Act (ITADA), which criminalized identity theft and established penalties of up to 15 years imprisonment and a $250,000 fine. ITADA designated the Federal Trade Commission (FTC) to coordinate efforts by law enforcement agencies across the nation to track down and prosecute identity thieves.

In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA). FACTA amended 15 U.S. Code §1681a to define the term "identity theft" as "a fraud committed or attempted using the identifying information of another person without authority."

In addition, FACTA amended the Fair Credit Reporting Act (FCRA) to provide expanded protection for victims of identity theft. The FCRA, as amended by FACTA, requires credit reporting agencies and creditors to help victims recover from identity theft by allowing consumers: (1) to place fraud alerts on their credit files if they are or believe they may become victims of identity theft; (2) to dispute inaccurate information; and (3) to receive a free credit report once per year from each of the three credit reporting agencies. Additionally, the law requires credit reporting agencies and creditors to investigate identity theft claims and correct

relevant information. FACTA also requires financial institutions to establish programs designed to address identity theft (the "Red Flag Rule"). Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft.

In 2004, the Identity Theft Penalty Enhancement Act became law. This Act established enhanced penalties for "aggravated" identity theft, which consists of using another's identity to commit felony crimes, including immigration violations, theft of another's Social Security benefits, and acts of domestic terrorism.

In 2008, the Identity Theft Enforcement and Restitution Act became law. This Act amended federal law regarding orders of restitution to clarify that the amount of restitution in an identity theft case may include the value of the victim's time that was spent remediating the actual or intended harm of the identity theft. In addition, this Act removed the prior jurisdictional restriction regarding computer intrusion crimes that had permitted the federal district courts to hear only those cases where state lines had been crossed in the commission of the crime.

State Identity Theft Statutes

Today, every state plus the District of Columbia has a statute that criminalizes identity theft, although there is some variation among the approaches. By example, twenty-nine states address restitution for victims of identity theft crimes, and five states have provisions that provide for the forfeiture of any property received or used in connection with an identity theft crime. It should also be noted that many states have heightened penalties if the victim is a senior citizen or disabled person, which may be increased if the identity thief served as the victim's caretaker.

Tax Preparer Penalties for Client Information Disclosure

In addition to penalties for identity theft, Internal Revenue Code Sections 6713 and 7216 provide for monetary and criminal penalties on unauthorized disclosures or use of taxpayer information by a person engaged in the business of preparing or providing services in connection with tax return preparation. States similarly impose civil and/or criminal penalties against certified public accountants (CPAs) and other tax preparers who fail to properly protect their clients' personal information.

Enforcement Developments

The IRS estimated that during the 2013 filing season alone, over 5 million tax returns were filed using stolen identities, claiming approximately $30 billion in refunds. The IRS was able to stop or recover over $24 billion of that total, or approximately 81% of the fraudulent claims. The collaboration between the IRS, the Department of Justice, Tax Division (DOJ-Tax) and United States Attorney's Offices have contributed to this success.

> "2,416,773 taxpayers were affected by identity theft in 2013, nearly double the number of victims in 2012"

DOJ-Tax, Directive 1441 specifically focuses on identity theft in the context of fraudulent tax refunds and provides for a streamlined investigation and prosecution process. Directive 144 also addresses Stolen Identity Refund Fraud (SIRF), in which perpetrators typically file false returns electronically, early in the tax filing season so that the IRS receives the false SIRF return before legitimate taxpayers have time to file their returns. The SIRF perpetrators arrange to have the refunds electronically transferred to debit cards or delivered to addresses where they can steal the refund out of the mail.

DOJ-Tax established an Advisory Board of experienced prosecutors to develop and implement uniform national policies for fighting SIRF crimes. By example, the Division works closely with the IRS to quickly share information obtained from SIRF investigations and prosecutions, which the IRS can use to make it more difficult for the schemes to be successful by blocking the false claims for refunds from being paid.

Validation Efforts

On June 11, 2015, the IRS joined representatives of tax preparation and software firms, payroll and tax financial product processors, and state tax administrators to announce a collaborative effort to combat identity theft and refund fraud. The new measures include steps to validate taxpayer and tax return information at the time of filing.

On August 12, 2015, in an effort to curb the ability of tax identity thieves to obtain fraudulent refunds by filing false returns early in the filing season, the IRS issued temporary regulations which eliminated an automatic deadline extension that had been available to companies filing their employees' Form W-2s. The next day, the IRS issued Announcement 2015-22, which clarified that individuals who receive identity protection services because their personal information may have been compromised in a data breach need not include in gross income the value of the identity protection services provided by an organization that experienced the data breach.

Best Practices to Deter Identity Theft

There are simple and worthwhile precautions that individuals can take to minimize the vulnerability of personally identifiable information. And should identity theft prove inevitable, even despite best practices, following tips such as reviewing monthly bank statements, obtaining a credit report at least once a year, etc., will allow an individual to notice fraudulent activity when it begins, which is key to a swift response that will contain the extent of the fraud and minimize the damage.

Some Best Practices for Protecting Personally Identifiable Information

- Secure personal information in the home and workplace. This includes shredding documents that contain personally identifiable information, such as bank statements.

© 2015 CCH Incorporated and its affiliates. All rights reserved.

- Protect personal computers using firewalls, antivirus software, and security patches.
- Secure wireless networks.
- Create strong passwords and frequently change them.
- Double-check a website's URL before entering any personal information. For example, confirm that a page that appears to be a government website is followed by .gov.
- Do not close a browser before logging out of a website.
- Encrypt and password protect sensitive documents.
- Check for a "lock" icon on the status bar of your Internet browser, which means your information should be safe when it's transmitted.
- Set online account settings that send an email or text message if someone attempts to log on to an account from an unrecognized computer or change a password.
- Put passwords on all of your credit card and bank accounts.
- Consider identity theft detection services, which include Lifelock and IdentityForce.

Identity Theft Indicators and Responses

People are generally familiar with the multitude of signs of non-tax related identity theft, including unfamiliar credit card charges, unexpected cards arriving, and overdrawn bank accounts. However, individuals may be less familiar with the signs of tax-related identity theft.

Top Indicators of Tax-Related Identity Theft

According to the Taxpayer Advocate Service (TAS), the most common indicators that an individual is a victim of tax-related identity theft are:

- A taxpayer attempts to file a return electronically, but the IRS rejects the return stating that another return with the taxpayer's SSN has already been filed;
- A taxpayer receives an IRS notice indicating that wages were received from an establishment at which the taxpayer never worked;
- A taxpayer receives a letter from the IRS indicating either that: (1) a return has already been filed, when the taxpayer has not yet filed a return; or (2) multiple returns have been filed; or
- A taxpayer receives a balance due notice, refund offset notice, or collection actions taken against the taxpayer regarding a year for which no return was filed nor refund received.

Steps to Take When Identity Theft is Suspected

Once an individual learns that his or her personally identifiable information has been compromised, there are certain steps that one can immediately take in order to prevent, or at least contain, fraudulent misuse.

- File a report with the FTC.
- File Form 14039 with the IRS.
- Contact the IRS Identity Protection Specialized Unit at (800) 908-4490.
- Immediately replace lost or stolen government identification (i.e., passport, driver's license).
- Immediately replace lost or stolen credit, debit, and charge cards.
- Immediately change logins, passwords, and PINs for compromised accounts.
- Obtain a current credit report.
- Call the fraud departments at any credit card, cell phone, or other businesses where accounts may have been compromised to get records regarding the identity theft.
- Challenge liability for any unauthorized transactions.
- Freeze or close the accounts at issue so that charges may only be approved with the individual's authorization.
- Contact the credit reporting agencies and have a Fraud Alert added to your credit report.
- Send a copy of the completed Identity Theft Report to the credit reporting agencies and request that each block any fraudulent transactions from appearing on a credit report.

Responses Specific to Tax-Related Identity Theft

There are additional steps that a victim of tax-related identity theft should take to correct the individual's tax account and prevent further misuse.

- Complete an FTC Identity Theft Affidavit.
- Bring the completed FTC Identity Theft Affidavit to the local police department, and file a police report.
- File an online complaint with the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov.
- Create an Identity Theft Report by combining Identity Theft Affidavit with police report.
- File IRS Form 14039 Identity Theft Affidavit and select the box that states "I am a victim of identity theft AND it is affecting my federal tax records."
- Contact the IRS Identity Protection Specialized Unit by phone at (800) 908-4490.
- If an IRS Letter 5071C is received, the taxpayer's identity may have been compromised. Recipients must verify their identities by calling the number on the letter, or by using the IRS's online Identity Verification tool, available online at: https://idverify.irs.gov.
- If an IRS Letter CP01A or CPO1F is received, the taxpayer has been identified as a possible identity theft victim and may request an IP PIN to further protect the taxpayer's account from tax-related identity theft.