Receive a Completely Unexpected "IRS" Tax Refund in Your Bank Account? STOP!!! Don't Take the Bait!

By Tom Bassett, J.D., CPA

Trending Upward Again in 2018 – Taxpayer Identity Theft

As head of Commerce Trust Company's East Region tax group, Tom Bassett, J.D., CPA, takes a moment to share his bird's eye view of the new tactics electronic thieves are using to steal money from federal tax filers.

Commerce Brokerage Services, Inc.
A Subsidiary of Commerce Bank

Q. As tax season gets into full swing, what are you seeing as the top issue for tax preparers and tax filers this year?

A. There are new twists on what is unfortunately a constant problem now – taxpayer identity theft. Cyberthieves have evolved and unfortunately gotten better. Stolen identity refund fraud has taken a new form to fool the unwary.

Q. How have cyberthieves changed their tactics?

A. In the recent past, the bad guys would use your stolen identity to file fraudulent claims for refunds and then have the proceeds sent directly to them on debit cards. Now they've discovered it's better to have the refund direct-deposited to an unwitting filer's bank account. Soon after the unexpected deposit arrives, the cyberthieves call posing as IRS representatives or collection agencies to pressure the filer on the phone to wire the "mistaken" refund back to them at a specified address.

Q. Why do people respond to this?

A. The bad guys know exactly how much was deposited into a recipient's account and they spin a credible story that this refund "error" has to be returned immediately

or the IRS will levy stiff penalties. Recipients know they did not deposit the money themselves and it shouldn't be in their accounts. It ends up being a credible spoof because no one wants to get sideways with the IRS, so filers get nervous and follow the fraudulent instructions.

Q. What should filers do if they get a suspicious phone call or a voice mail regarding a potentially fraudulent refund?

A. Ask the caller to give you a number where he or she can be reached, note the time of day, and politely say you'll return the call after you've consulted with your tax advisor. Do not get flustered or withdraw the funds if they are in your account. Take the time to speak directly with your bank representative or the IRS first. If you make the mistake of wiring the money to the thieves, you unwittingly become complicit in the ruse. By voluntarily sending the refund back, you lose your leverage on potential recovery of the theft. It's a diabolically clever scam.

Q. What happens next if you've sent the money?

A. Unfortunately, nothing good. The IRS will likely call you requesting return of the funds because they will

automatically know you haven't filed your taxes yet. If you've already voluntarily sent "erroneous refund" to the cyberthieves, you've lost the proceeds that still rightfully belong to the IRS. So the IRS will want the refund back and your ability to seek redress through the IRS or the bank is compromised. The cyberthieves know this and capitalize on the confusion of who might be liable.

Q. What does the IRS recommend taxpayers do if their return has been compromised?

A. The IRS encourages taxpayers to discuss the issue with their financial institutions because they may need to close bank accounts. Taxpayers receiving erroneous refunds should also contact their tax preparers immediately. There are established procedures they should follow to return erroneous funds. One important procedure, for example, is to send only paper checks. Taxpayers who receive a direct deposit refund that they did not request should take the following steps:

1. Contact the Automated Clearing House (ACH) department of the bank/financial institution where the direct deposit was received and have them return the refund to the IRS.

2. Call the IRS toll-free at 800-829-1040 (individual) or 800-829-4933 (business) to explain why the direct deposit is being returned.
3. Keep in mind interest may accrue on the erroneous refund.

There is more information at https://www.irs.gov/taxtopics/tc161.

Q. How extensive is refund fraud in general?

A. Despite the preventive measures taken over the last two years, the IRS estimates it paid out $1.3 billion in fraudulent tax refunds in 2017. However, the number of taxpayers reporting to the IRS that they are victims of identity theft is declining. The IRS said that it received 242,000 reports from taxpayers in 2017 compared to 401,000 in 2016 – a 40 percent decline. It's lessening, but still a serious drain on our national resources.

Q. What is the IRS doing about the problem?

A. As one recent example, the IRS worked with large companies to add a code in Box 9 of the standard W2 form that helps corroborate your identity information when you submit your taxes. IRS officials are also

focusing on strengthening safeguards tax preparers employ – when tax preparers are hacked, the trouble expands exponentially.

Q. Would it be better to file on paper vs. electronically?

A. It makes no difference on your chances of being defrauded. The cyberthief is simply interested in getting to your employer deposits credited to your IRS account (your withholding and any prepayments) before you do. If you try to electronically file your return, you will get immediate feedback that your Social Security Number has been compromised, whereas if you paper file, it could be months before the IRS inputs your return, and months before they tell you your account has been compromised.

Key Takeaways

- Everyone must be vigilant and alert – both taxpayers and tax professionals.

- Never take an email from a familiar source at face value. For example, an email from "IRS e-Services" could be a bogus email address. If it asks you to open a link or attachment, or threatens to close your

account, think twice. Hover your cursor over the link to see the real web address (URL). If you don't recognize it, do not open.

- Use security software. Always use security software with firewall and anti-virus protections. Make sure the security software is always turned on and can automatically update. Encrypt sensitive files, such as tax records, stored on computers. Use strong, unique passwords for each account.

- Watch out for scams. Learn to recognize and avoid "phishing" emails and threatening calls and texts from thieves posing as legitimate organizations such as banks, credit card companies, tax software firms, or even the IRS. Do not click on links or download attachments from unknown or suspicious emails.

- Protect personal data. Don't routinely carry Social Security cards and make sure tax records are secure. Shop at reputable online retailers. Treat personal information like cash; don't leave it lying around.

For more information, see www.irs.gov/identitytheft.

The 2018 investment commentary is a special report designed to provide investment information on economic markets for Commerce Brokerage clients. It is intended to provide general information only and reflects the opinions of Commerce Trust Company's Investment Policy Committee.

Commerce Trust Company is a division of Commerce Bank. Commerce Brokerage Services, Inc., member FINRA and SIPC, and an SEC registered investment advisor, is a subsidiary of Commerce Bank.

This material is not a recommendation of any particular security, is not based on any particular financial situation or need, and is not intended to replace the advice of a qualified attorney, tax advisor or investment professional. The information in this commentary should not be construed as an individual recommendation of any kind. Strategies discussed here in a general manner may not be appropriate for everyone. Diversification does not guarantee a profit or protect against all risk. Past performance is no guarantee of future results, and the opinions and other information in the investment commentary are as of March 20, 2018.

Commerce does not provide tax advice or legal advice to customers. Consult a tax specialist regarding tax implications related to any product or specific financial situation. Data contained herein from third-party providers is obtained from what are considered reliable sources. However, its accuracy, completeness or reliability cannot be guaranteed. All expressions of opinion are subject to change without notice depending upon worldwide market, economic or political conditions.

commercebank.com/brokerage

1.800.772.7283

NOT FDIC INSURED | MAY LOSE VALUE | NO BANK GUARANTEE

THOMAS BASSETT, J.D., CPA

Vice President, Tax Manager – East Region

Tom has managed the East region tax team for Commerce Trust Company since joining in 2012. He is responsible for the services his department provides to clients of Commerce Trust in the St. Louis, Springfield, Belleville, Peoria, and Bloomington offices. In addition to tax planning and consulting services to that client base, his group annually prepares more than 120 returns for charitable trusts and private foundations and more than 350 returns for individual, estate, gift, trust, and partnership clients of Commerce Trust. Tom also co-manages Commerce Trust's annual tax return preparation process, including reviewing and maintaining Commerce Trust's accounting system and the integration of this system with the organization's external vendor. Tom attended Washington University in St. Louis, earning two bachelor of arts degrees in physics and psychology, a juris doctorate, a master of business administration, and a master of science in business administration. He is a member of the Missouri Society of Certified Public Accountants, the American Institute of Certified Public Accountants, the Missouri Bar Association, The Bar Association of Metropolitan St. Louis, the American Association of Attorney-Certified Public Accountants, and the Estate Planning Council of St. Louis. Tom has chaired the audit, investment, and budget subcommittees of the Finance Committee of The Bar Association of Metropolitan St. Louis for several years.

Commerce Brokerage Services, Inc.
A Subsidiary of Commerce Bank

commercebank.com/brokerage

1.800.772.7283

NOT FDIC INSURED | MAY LOSE VALUE | NO BANK GUARANTEE