Tax Insights

Helping You Succeed

ACCUITY

FEBRUARY 3, 2022

Tax-related identity theft continues to be an ever-growing global crisis

We want to share with you some proactive steps and resources to help in your defense against tax-related identity theft.

Suggestions to protect you and your family from identity theft

Secure private personal information. Safeguard family names and birthdates, account numbers, passwords and Social Security numbers. Carefully consider all requests to provide your Social Security number before giving it out and don't hesitate to ask why your private information is being requested. Secure your Social Security card in a safe or safety deposit box and never in your purse or wallet. Proactively shred all documents that contain personal data before disposing of them, even solicitations and "junk" mail that may unknowingly contain account numbers and personal information.

Monitor personal information shared on social media. Cybercriminals methodically gather data from online sources, including commonly used identifiers such as birthdate, maiden name, pet name, hometown, significant other and/or children's information. Be cautious who you communicate with online and be selective before accepting electronic invitations from people you do not know or recognize. Separate what you post publicly from what you post with your personal contacts. Do not post personal and family data and set your account to private so it is not freely accessible to the public.

Secure your computer. Use current versions of antivirus, malware protection and firewalls and update these programs frequently. Consider having your software updated automatically, as well as using different computers for business and finances than you do for social media and personal matters. Use strong passwords, change them frequently and do not share them with others. Review IRS Publication 4524, *Security Awareness for Taxpayers*, for additional tips.

Beware of impersonators. Criminals utilize sophisticated computer technology, such as dialers and automated questions, to contact thousands of targets daily. Do not provide personal information to callers you do not know. If any caller requests that you verify personal information, be extremely cautious and ask for further confirmation of their identity, such as their telephone number, website, email address, supervisor's name and mailing address. The IRS never initiates contact by telephone.

Beware of unsolicited emails and current phishing scams. Don't open attachments or electronic links unless you know the sender. Internet sites should have a lock symbol to show the site is encrypted. Always beware of entering sensitive data. Forward emails received from IRS impersonators to phishing@irs.gov. The IRS never initiates contact by email, text message or social media channels. For more guidance on phishing scams, go to irs.gov/privacy-disclosure/report-phishing.

Monitor your personal information. Review your bank and credit card statements often. Immediately investigate any unusual activity.

Suggestions to protect you and your family from identity theft (continued)

Consider electronic transmission of financial information. No sensitive tax or personal information should be sent via unsecured email, even information being transmitted to CPAs, bankers or other financial advisors. A secure portal, encrypted email or physical mailing of sensitive information is necessary.

Order your free annual credit report. Call (877) 322-8228 or go to annualcreditreport.com to request your report and/or search for creditors you do not know. Choose to use only the last four digits of your Social Security number on your report. Consider placing a credit card freeze on your account so only creditors you approve can access your file.

What to do if you become a victim of tax-related identity theft

You may learn that your identity has been compromised by receiving a letter in the mail from the IRS, or when your personal income tax return is electronically submitted and subsequently rejected. If you receive a notice indicating identity theft, contact your CPA immediately so that appropriate steps can be taken to resolve the matter.

Other ways you may discover your identity has been stolen include:

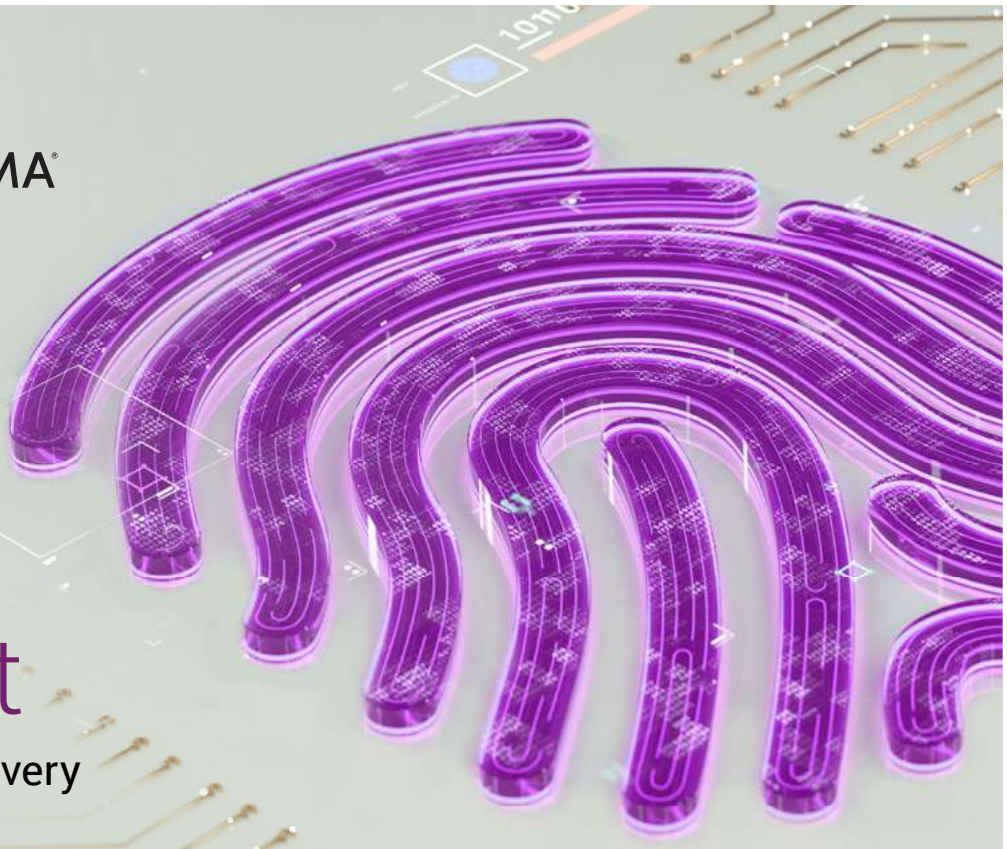
- Finding purchases on your credit card that you did not make
- Discovering withdrawals from an account that you did not make
- Seeing that your address has been changed for certain accounts or you are no longer receiving your regular bills. (Cyber criminals may change your address when filing a return.)
- A letter or email from a business you are associated with (such as your cell phone provider) letting you know that they have been subject to a computer hack

The unfortunate reality is that personal data is already at risk everywhere, but you can take steps to reduce the likelihood of you being victimized by cyber criminals.

Please see the attached copy of the AICPA & CIMA Identity Theft Checklist which outlines action steps you and your organization may take to combat identify theft.

If you have any questions, please contact us.

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting or tax advice. This communication may not be applicable to your specific circumstances and may require consideration of non-tax and other tax factors if any action is to be contemplated. Please contact your tax professional prior to taking any action based on this information. Accuity LLP assumes no obligation to the reader of any changes in tax laws or other factors that could affect the information contained herein.



Identity Theft Checklist

Action steps for recovery

Identity theft is a complex and evolving global threat. Without question, it is one of the most pressing challenges our world faces.

Unfortunately, the COVID-19 pandemic exacerbated the growing problem. Fraudsters continue to look for new ways to steal confidential information to commit crimes. As your trusted tax and financial adviser, we understand your concerns with identity theft and take every precaution to keep your personal information safe.

There are numerous types of identity theft. For example, a thief could steal a wallet and use credit cards to make illegal purchases or obtain information to file a tax return on behalf of a taxpayer to claim an illegal refund.

Should you become a victim of any type of identity theft, the checklist on the next two pages will be your guide. It outlines specific steps you should take to help mitigate the damage of identity theft: closing credit cards, filing a police report, filing a complaint with the Federal Trade Commission (FTC), addressing matters with the IRS and more.

For tax-related identity theft matters, we are here to help. Assistance may involve contacting the IRS to make sure your payments are properly credited to your account, helping to retrieve a refund issued to the wrong person or responding to IRS notices. Feel free to call our office to discuss your situation and see how we can be of service.

Reviewed Dec. 1, 2021

Combating identity theft

Organization	What to do
Companies where you know fraud occurred (including debt collectors)	☐ Contact the fraud department of each company where the fraud occurred and explain that your identity was stolen. Ask them to freeze or close the account and not add any new charges unless you agree. Document your phone conversation, including the name of the person with whom you speak. Also, ask them to send you a letter confirming you are not liable for the fraudulent activity. ☐ Change your logins and passwords, as applicable. Note: You may need to contact these companies again after you receive an Identity Theft Report from the FTC.
Credit agencies	☐ Report the identity theft to the fraud department of one of the following reporting agencies as soon as possible. They must notify the other two agencies. • Equifax: equifax.com • Experian: experian.com • TransUnion: transunion.com ☐ Request a copy of your credit report and that only the last four digits of your Social Security number be placed on the report. ☐ Inform the credit bureaus and the credit issuers (in writing) of any fraudulent accounts and incorrect information. ☐ Obtain replacement credit cards with new, secure account numbers and destroy any old cards. ☐ Notify those who have received your credit report in the last six months to alert them to any disputed, fraudulent or incorrect information. ☐ Ask for a free, one-year fraud alert by contacting one of the three credit bureaus. That company must inform the other two. You will get a letter from each credit bureau that will confirm they placed a fraud alert on your file. ☐ Request and confirm that an extended fraud alert (seven years) is placed on your credit report.
Federal Trade Commission (FTC)	☐ Report the crime to the FTC. Note: The FTC has overhauled the process for helping victims of identity theft. Go to identitytheft.gov to report identity theft. ☐ Based on the information you provide, identitytheft.gov will create your Identity Theft Report and recovery plan. ☐ Verify that the report lists the fraudulent accounts and keep a copy of the report.
Local police	☐ Report the crime to your local police or sheriff's department. Make sure to provide as much documented evidence as possible.
Health insurance providers	☐ Contact your health insurance company if your insurance card was accessed or stolen to help prevent the thief from using your insurance. Similarly, notify Medicare if your Medicare card was accessed or stolen.

Combating identity theft *(cont.)*

Organization	What to do
Internal Revenue Service (IRS)	☐ Contact the IRS to report tax-related identity theft. This will alert them to any refund claim or other activity on your account. File IRS Form 14039, *Identify Theft Affidavit*. • Call the IRS Identity Protection Specialized Unit (IPSU) at 800.908.4490. Contact your CPA with any questions. • If you're a confirmed victim of tax-related identity theft, the IRS will mail you a letter with your Identity Protection PIN (IP PIN). It's important to keep this letter and provide a copy to your CPA. You may also request an IP PIN as a proactive measure to protect yourself against tax-related identity theft. See Get An Identity Protection PIN on irs.gov. • Contact your CPA with any questions and for help filing Form 14039 or obtaining an IP PIN.
State tax agencies	☐ Contact applicable state tax agencies to report related thefts and identity theft issues. Some agencies may require a police report and/or the IRS affidavit.
Utilities and brokers	☐ Contact your local utility providers (gas, electric, cable, internet, cellular carrier, etc.) to make sure no new accounts were opened in your name. Similarly, let your investment or retirement account company know your identity documents were stolen so they will be alert to any suspicious activity on your account.
Other agencies and organizations	☐ For U.S. mail fraud, contact your local postal inspector. • Online: uspis.gov/report • Phone: 877.876.2455 ☐ For Social Security number misuse (non-IRS issues): Check your earnings record to make sure no one is using your identification number to obtain work. Call your local Social Security Administration (SSA) office if something looks inaccurate. Contact the SSA Inspector General to report Social Security benefit fraud, employment fraud or welfare fraud. • Online reporting resources: – oig.ssa.gov – Fraud Reporting Form • SSA fraud hotline: 800.269.0271 • Apply for a replacement Social Security card if your card was lost or stolen. ☐ If your driver's license was lost or stolen, contact the nearest Department of Motor Vehicles (DMV) branch to report it. ☐ If your passport was lost or stolen, call the State Department at 877.487.2778.

Combating identity theft *(cont.)*

What else can you do?

- Create an identity theft file (keep copies of everything).
- Change all your account passwords. As an extra step, consider changing your username. Be sure to use strong passwords.
- In all communications with the credit bureaus, refer to the unique number assigned to your credit report. When mailing information, use a certified return receipt. Be sure to save all credit reports as part of your fraud documentation file.
- Review your credit report periodically. An extended fraud alert allows you to obtain two free credit reports from each of the credit reporting agencies within 12 months.
- Consider requesting a security freeze. By freezing your credit reports, issuers can't access your credit files without your permission. This prevents thieves from opening new credit card and loan accounts.
- Consider requesting a criminal background check to confirm your identity is not being used in connection with criminal activities.

Should you need assistance, please contact our office. Our trained staff is available to help you resolve identity theft matters (including problems with the IRS) and proactively make sure your information is secure.

Contact information

Address Accuity LLP, 999 Bishop Street, Suite 1900, Honolulu HI 96813

Phone number 808-531-3400

Website accuityllp.com

This copyrighted resource is provided exclusively to AICPA® Tax Section members and should not be shared, reproduced or used by anyone who is not a member of the AICPA Tax Section without explicit consent from the AICPA Tax Section. See our terms and conditions. For information about content licensing, please email copyrightpermissions@aicpa-cima.com.

AICPA & CIMA

© 2021 Association of International Certified Professional Accountants. All rights reserved. AICPA and American Institute of CPAs are trademarks of the American Institute of Certified Public Accountants and are registered in the US, the EU and other countries. The Globe Design is a trademark owned by the Association of International Certified Professional Accountants and licensed to the AICPA. 2111-43628