

Monthly Newsletter - February 2021

In This Issue

- Organizers Have Been Created and Mailed
- Engagement Letters Have Been Mailed
- All Taxpayers Are Now Eligible for Identity Protection PINs
- Be Prepared for These Pandemic-Related Tax Surprises
- Your Identity is NOT Your Own

Organizers Have Been Created and Mailed

Your 1040 Organizer was sent to your Coleman Portal on January 20th. The email notification was from info@colemancpas.com.

Paper Organizers were mailed on January 21st.

Please be sure to read the 2020 Cheat Sheet for the information required to begin processing your tax return.

Engagement Letters Have Been Mailed

All 1040 engagement letters were mailed on January 20th. Portal users, the engagement letters are not on your portal.

***NEW* - Married couples must both sign the engagement letter.**

Please be sure to read the 2020 Cheat Sheet for the information required to begin processing your tax return.

All Taxpayers Are Now Eligible for Identity Protection PINs

The IRS has expanded the Identity Protection PIN Opt-In Program to all taxpayers who can verify their identity.

If you adjusted gross income is greater than \$72,000, then you need to make an in-person appointment at an IRS office to verify your identity and obtain an IP PIN.

The Identity Protection PIN is a six-digit code known only to the taxpayer and to the IRS. It helps prevent identity thieves from filing fraudulent tax returns using a taxpayers' personally identifiable information.

Here are a few key things to know about the IP PIN Opt-In program.

- This is a voluntary program.
- Taxpayers must pass a rigorous identity verification process.
- Spouses and dependents are eligible for an IP PIN if they can verify their identities.
- An IP PIN is valid for a calendar year.
- People must get a new IP PIN each filing season.
- The online IP PIN tool is offline between November and mid-January each year.
- Correct IP PINs must be entered on electronic and paper tax returns to avoid rejections and delays.
- Taxpayers should never share their IP PIN with anyone but their trusted tax provider.
- The IRS will never call, text or email requesting their IP PIN.
- People should beware of scams to steal their IP PIN.
- There currently is no opt-out option but the IRS is working on one for 2022.

How to get an IP PIN

Taxpayers who want an IP PIN for 2021 should use [Get an IP PIN](#) tool on IRS.gov. This tool uses Secure Access authentication verify a person's identity. Taxpayers should review the [Secure Access requirements](#) before they try to use the Get An IP PIN tool. There is no need to file a Form 14039, Identity Theft Affidavit, to join the program.

Once a taxpayer has authenticated their identity, their 2021 IP PIN immediately will be revealed to them. This PIN must be used when prompted by electronic tax returns or written near the signature line on paper tax returns.

Options for taxpayers who can't verify their identity online

Taxpayers whose adjusted gross income is \$72,000 or less may complete Form 15227, *Application for an Identity Protection Personal Identification Number*, and mail or fax it to the IRS. A customer service representative will contact the taxpayer and verify their identity by phone. Taxpayers should have their prior year tax return for verification process.

Taxpayers who verify their identity this way will have an IP PIN mailed to them the following tax year. This is for security reasons. Once in the program, the IP PIN will be mailed to these taxpayers each year.

Taxpayers who can't verify their identity online or by phone and are ineligible for file Form 15227 can contact the IRS and make an appointment at a Taxpayer Assistance Center to verify their identity in person. They'll need to bring should bring two forms of identification, including one government-issued picture identification.

Taxpayers who verify their identity in-person will have an IP PIN mailed to them within three weeks. Once in the program, the IP PIN will be mailed to these taxpayers each year.

Confirmed identity theft victims

Current tax-related identity theft victims who have been receiving IP PINs by mail will experience no change.

Taxpayers who are confirmed identity theft victims or who have filed an identity theft affidavit because of suspected stolen identity refund fraud will automatically receive an IP PIN by mail once their cases are resolved.

Be Prepared for These Pandemic-Related Tax Surprises

Don't get shocked by a high tax bill! Be prepared for these pandemic-related tax surprises when you file your 2020 tax return.

- ✓ **Taxes on unemployment income.** If you received unemployment benefits in 2020, you need to report these benefits on your tax return as taxable income.
- ✓ **Taxes from side jobs.** Did you pick up a part-time gig to make ends meet? Payments received for performing these jobs may not have had your taxes withheld.
- ✓ **Unusual profit-and-loss.** If you run a business that was hit by the pandemic, you may find your estimated tax payments were either overpaid or underpaid compared to normal.
- ✓ **Underpayment penalty.** If you did not have proper tax withholdings from your paycheck or your estimated tax payments weren't enough, you could be subject to an underpayment penalty.
- ✓ **A chance to claim missing stimulus payments. (A good surprise!)** If any of your stimulus payments were for less than what you should have received, you can get money for the difference as a tax credit when you file your 2020 tax return.

Your Identity is NOT Your Own

How companies use your identity and what you can do to protect it.

One of the most valuable things you own is YOU. Your identity includes the basics - where you live, your age, and your gender. But it also includes your interests, who you know, and what you buy. So, do you know who has your identity? Here's the life cycle of your identity and what to do to protect it.

- **It gets collected.** Think about the organizations that legally collect information about your identity – your employer, government entities, insurance companies, banks, credit reporting agencies, and non-profit organizations. And then add those companies you give your identity to freely - like Google, Facebook, LinkedIn, Twitter, and any other website or social media platform you visit.
- **It gets stored.** Once your identity gets collected, it then needs to be stored somewhere. Storage is most often on servers or locally on a computer or mobile device. This is one of the core concerns with Tik-Tok, a Chinese-originated short video service. The concern is that a

foreign entity will have stored U.S. citizen's interests and behaviors that can help identify potential targets that can be manipulated.

- **It gets sold.** Once information related to your identity and interests are collected, most organizations then sell it to other companies. Not only is information about your identity sometimes collected without your knowledge, this information is then monetized. Your viewing behavior can also be actively manipulated by the sites you view. If you read articles about cats, you are going to get a lot more articles about cats and get ads that relate to cat-lover behavior. This is often so subtle, you do not realize it is happening.
- **It gets accessed.** If your information is considered a public record, anybody can see it. Business licenses, property tax records and real estate ownership are just a few examples of personal information that anyone can access.
- **It gets stolen.** Identity thieves are always looking for ways to access your information. Thieves either hack one of the organizations that collects your confidential information or find a way to trick you into giving them your information, with techniques such as phishing emails.

What you can do

- **Opt-out of providing personal information.** The best place to start with protecting your identity is knowing who has access to it and asking if they really need it. Consider opting out of providing information if possible.
- **Be vigilant with the data you possess.** While you can't control how secure an insurance company's servers are, you can control how secure you handle the information and documents you possess. Be on the lookout for phishing emails, verify requests for your information and don't forget about getting rid of documents the old-fashioned way with a shredder.
- **Deliberately monetize your identity.** Stop giving away your identity without a thought. Here's an idea. Consider you are worth a million dollars. Then see what these services are paying you for your information and how they are using it. If this little exercise gets you to pause before signing up for a new service, then the exercise is worth it!

As always, contact the office with questions by emailing us at info@colemancpas.com or calling 773-444-3100. We are here to help.

This publication provides summary information regarding the subject matter at time of publishing. Please call with any questions on how this information may impact your situation. This material may not be published, rewritten or redistributed without permission, except as noted here. This publication includes, or may include, links to third party internet web sites controlled and maintained by others. When accessing these links the user leaves this newsletter. These links are included solely for the convenience of users and their presence does not constitute any endorsement of the Websites linked or referred to nor does COLEMAN & ASSOCIATES CPAs LTD have any control over, or responsibility for, the content of any such Websites. All rights reserved.