Coleman & Associates
Fully Integrated Tax, Accounting & Financial Services

Monthly Newsletter - December 2020

In This Issue

Important Dates & Deadlines to Note

January 15

- ❖ 4th quarter estimated payments due

Unemployment Fraud: A Message to Illinois Employers

On November 4, 2020, the Illinois Department of Employment Security emailed the following regarding fraudulent unemployment claims:

Nationwide, bad actors are using the COVID-19 pandemic as an opportunity to file fraudulent claims for unemployment insurance benefits. Many of these claims involve the theft of employees' identities. Personal information has been stolen from many different sources in the past years, including computer hacks into the databases of some of the largest companies in the nation. This information can be used to file fraudulent unemployment claims.

It is likely that as an employer, you have recently seen an increase in fraudulent unemployment claims. You are not alone – this has been happening across the country. IDES is partnering with federal, state, and local law enforcement agencies in response. IDES is also partnering with employers to stop fraudulent claims in their tracks. If you receive a Notice of Claim informing you that an individual with a given name and social security number has filed a claim for benefits, please confirm if that individual is still working for you. If so, please ask whether that individual did, in fact, file a claim. We ask that you report to IDES as soon as possible what information you have obtained.

The best way to report fraudulent claims to IDES is by filing a timely protest to a Notice of Claim, giving IDES as much useful information as you can.

Additionally, IDES has an established unit that works specifically on allegations of fraudulent claims. On each day that you are made aware of the possibility of a fraudulent claim, we ask that in addition to filing a timely protest, **you send one email with a spreadsheet** including the following information for each instance of suspected fraud from that day:

- The claimant's first name and last name

- The employer name
- The claim ID

All this information is shown on the Notice of Claim. Please send your email to both marco.morales@illinois.gov and gilbert.muniz@illinois.gov. Again, please ensure this information is included in a spreadsheet attachment – not the body of the email.

Best Practices To Create a Strong Password

The pandemic has become every hacker's dream as more people have been forced online to do everyday tasks such as shopping, banking and working from home. Strong and unique passwords are more important now than ever before. Hackers, with the aid of password crackers, use different methods to identify your password from the data that is stored in or transmitted by computer systems. Many of the password cracking techniques are successful due to weak or easily guessable passwords such as password123, admin, or failure to change the default password.

If you use an 8-digit password with upper, lowercase letters and numbers, it would take a password cracker alone over 35 years to figure out your password as there are over 218 trillion combinations. That sounds like a long time but this time is reduced significantly if you use common words or phrases. A hacker trolling your social media pages will try your significant other and children's names with a combination of birthdates, anniversaries, addresses, phone numbers or graduating class from college or high school.

So what makes a good password? By increasing your password to 12 digits including at least 1 special character, the password crackers detection time increases to 2.5 million years and 13.6 quintillion combinations if you do not use any specifically identifiable information. Make sure you choose 2-3 unrelated words and switch out a number or character for a letter(s) such as $taplerMa$kparr0t or p@per4c0rveTTe?

If this seems like too much to remember, check into a password manager such as Dashlane, 1Password, LastPass or Keeper. These services create random, high-strength passwords for all of your websites and applications and stores them in a secure, encrypted location. You'll only need to remember one password (and please don't put that on a post-it-note on your monitor or under your keyboard!)

Cybersecurity Tips for You and Your Employees

Working remotely is at an all-time high. The appropriate technology is in place to make it as safe as possible but often a key part of the process is overlooked – training your employees. Over the past several months we have attended multiple training courses and have compiled our top 10 cybersecurity tips to share with you.

1) Don't click on direct links in emails (phishing), text messages (smishing) or respond to telephone requests for sensitive information (vishing). If in doubt, call the number on your bank, credit card statement or invoice and not the phone number left for you in the message.
2) Never pay for any unexpected email request using a gift card. The IRS will never require you to pay an outstanding balance using gift cards.
3) Never respond to unsolicited emails or calls claiming to be from the IRS, Social Security and the state Department of Revenue. These entities always send their notices through the U.S. mail.

4) Social media and company websites are a great source for “spear-phishing” information about you, your family, friends and co-workers. Pick up the phone and call your boss or family member before you buy those surprise gift cards or wire funds to an unknown bank account. It’s better to be safe than sorry.
5) Never use one password for multiple websites. This is known as “credential stuffing” and allows hackers to gain access to other sites by using the same name and password.
6) Enable multi-factor authentication (MFA) whenever possible. More programs are adding this feature.
7) Always check the sender’s email address. Beware of any email addresses that have additional extension after the .com such as info.com.ru (originates from Russia).
8) Do not open any email attachments that end with .exe, .scr, .bat, or other executable files you do not recognize as these usually contain malware or ransomware which are downloaded to your computer.
9) Disable automatic Bluetooth pairing on your electronic devices such as smartphones and tablets.
10) Explain appropriate and inappropriate sharing of information when onboarding new employees.

Implement cybersecurity awareness training for your employees and encourage them to share the information with their family members. No matter if you are large or small, financially secure or a struggling company, there are many options available. There are services that will customize a security awareness program such as KnowBe4, and many of them offer free tools on their website.

The ultimate goal is to have everyone “Think before you CLICK!”

Employees: Don’t Forget About Your FSA Funds

Many employees take advantage of the opportunity to save taxes by placing funds in their employer’s health or dependent care flexible spending arrangements (FSAs). As the end of 2020 nears, here are some rules and reminders to keep in mind.

Health FSAs

A pre-tax contribution of $2,750 to a health FSA is permitted in both 2020 and 2021. You save taxes because you use pre-tax dollars to pay for medical expenses that might not be deductible. For example, they wouldn’t be deductible if you don’t itemize deductions on your tax return. Even if you do itemize, medical expenses must exceed a certain percentage of your adjusted gross income in order to be deductible. Additionally, the amounts that you contribute to a health FSA aren’t subject to FICA taxes.

Your plan should have a listing of qualifying items and any documentation from a medical provider that may be needed to get a reimbursement for these items.

To avoid any forfeiture of your health FSA funds because of the “use-it-or-lose-it” rule, you must incur qualifying medical expenditures by the last day of the plan year (Dec. 31 for a calendar year plan), unless the plan allows an optional grace period. A grace period can’t extend beyond the 15th day of the third month following the close of the plan year (March 15 for a calendar year plan).

An additional exception to the use-it-or lose-it rule permits health FSAs to allow a carryover of a participant’s unused health FSA funds of up to $550. Amounts carried forward under this rule are

added to the up-to-$2,750 amount that you elect to contribute to the health FSA for 2021. An employer may allow a carryover or a grace period for an FSA, but not both features.

Examining your year-to-date expenditures now will also help you to determine how much to set aside for next year. Don't forget to reflect any changed circumstances in making your calculation.

Dependent care FSAs

Some employers also allow employees to set aside funds on a pre-tax basis in dependent care FSAs. A $5,000 maximum annual contribution is permitted ($2,500 for a married couple filing separately).

These FSAs are for a dependent-qualifying child under age 13, or a dependent or spouse who is physically or mentally incapable of self-care and who has the same principal place of abode as the taxpayer for more than half of the tax year.

Like health FSAs, dependent care FSAs are subject to a use-it-or-lose-it rule, but only the grace period relief applies, not the up-to-$550 forfeiture exception. Thus, now is a good time to review expenditures to date and to project amounts to be set aside for next year.

Note: Because of COVID-19, the IRS has temporarily allowed employees to take certain actions in 2020 related to their health care and dependent care FSAs. For example, employees may be permitted to make prospective mid-year elections and changes. Ask your HR department if your plan allows these actions if you believe they would be beneficial in your situation. Other rules and exceptions may apply.

Contact us if you'd like to discuss FSAs in greater detail.

Check Out Our Blog

Did you know that we post additional tax, accounting, and financial updates to our blog each week? Check it out at https://colemancpas.com/blog

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