5525 Green Bay Road
Kenosha, WI 53144-3737

PARTNERS, L.L.C.
Certified Public Accountants
and Consultants

Telephone: 262/657-2060
Fax: 262/657-2080
www.ppgpartners.net

The 2017 Tax Season is Here!

Send Your 2016 Tax Information to PPG Partners
If PPG Partners is preparing your 2016 tax returns, please return your tax organizers with supporting documents (W-2s, 1099s, Social Security statements, bank/account statements, charitable donation receipts, etc.) to us if you have not yet done so. You don't have to wait to send in your information if you are still waiting on a couple of pieces of information – we can complete the majority of your tax return without them.

Maintain Tax Return Documents for 3+ Years
Even if your 2016 tax returns were accepted, don't throw out your documents just yet. Maintaining well-organized records will help provide answers if the IRS needs to follow-up with you for more information. You will want to keep the documents used to prepare your tax return for a minimum of three years (generally, the statute of limitations for the IRS to assess taxes on a taxpayer expires three years from the due date of the return or the date on which it was filed, whichever is later). This documentation now also includes your healthcare documents, such as records of any employer-provided coverage, premiums paid, the type of coverage, and Forms 1095.

Be Aware of Tax Scams

It's tax time, and that means tax scams are at their peak. Always keep in mind that the IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information. The IRS also does not threaten taxpayers with lawsuits, imprisonment or other enforcement action. Being able to recognize these telltale signs of a phishing or tax scam could save you from becoming a victim.

Common scams that have and continue to target taxpayers include: IRS-impersonation telephone scams; emailing, phishing and malware schemes; and tax refund scam artists posing as the Taxpayer Advocacy Panel.

Additionally, scammers are constantly identifying new tactics to carry out their crimes in new and unsuspecting ways. In recent years, the IRS has seen scammers use a variety of schemes to fool taxpayers into paying money or giving up personal information. Some of these new schemes include: soliciting W-2 information from payroll and human resources professionals, a fictitious "Federal Student Tax" scam targeting students and parents and demanding payment, automated calls requesting tax payments in the form of iTunes or other gift cards, and scammers pretending to be from the tax preparation industry.

Remember that:

- The IRS will never call you on the phone to demand immediate payment.
- The IRS will never call about taxes owed without first mailing you a notice.
- The IRS will never demand that you pay taxes without giving you the opportunity to question or appeal the amount the agency says you owe.
- The IRS will never require you to use a specific payment method for your taxes, such as a prepaid debit card.
- The IRS will never ask for credit card or debit card numbers over the phone.
- The IRS will never threaten to have you arrested for not paying.

Connect with PPG Partners Online!

twitter.com/**PPGPartners**

facebook.com/**PPGPartners**

linkedin.com/**company/ppg-partners-llc**

Penalties Increased for Failure to Post Labor Law Posters

The Department of Labor (DOL) has recently increased penalties by more than $500 for failure to display workplace labor law posters. On March 2, 2017, the maximum posting penalty from the DOL increased from $32,946 to $33,486.

Both state and federal labor law posters are required for businesses. If a business has one or more employees, it is required by the law to post federal, state and OSHA mandatory posters. More specifically, the following six postings must appear in each workplace location: federal minimum wage, Employee Polygraph Protection, OSHA, FMLA, USERRA, and EEO. If a business is not in compliance with current federal and state labor law poster standards, they are in jeopardy of receiving a fine or citation.

The posting regulations affected by increased penalties include the following:

- Family and Medical Leave Act (FMLA) - increased to $166
- Equal Employment Opportunity (EEO) - increased to $534
- Job Safety and Health: It's the law (OSHA) - increased to $12,675
- Employee Polygraph Protection Act (EPPA) - increased to $20,111

Five Ways to Protect Your Small Business from Account Fraud

(North Shore Bank) Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable. The following are tips to keep your small business safe.

Educate your employees. You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.

Protect your online environment. It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.

Partner with your bank to prevent unauthorized transactions. Talk to your banker about programs that safeguard you from unauthorized transactions. Positive Pay* and other services offer call backs, device authentication, multi-person approval processes and batch limits to help protect you from fraud.

Pay attention to suspicious activity and react quickly. Look out for unexplained account or network activity, pop ups, and suspicious emails. If detected, immediately contact your financial institution, stop all online activity and remove any systems that may have been compromised. Keep records of what happened.

Understand your responsibilities and liabilities. The account agreement with your bank will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a takeover.

*Positive Pay is an automated fraud detection tool offered at many banks. In its simplest form, it is a service that matches the account number, check number and dollar amount of each check presented for payment against a list of checks previously authorized and issued by the company. All three components of the check must match exactly or it will not pay. There is generally a bank fee for Positive Pay, although some banks now offer the service for free. Talk to your bank if you are interested in learning more about their Positive Pay options.