PenSoft® NEWS
Quarterly Newsletter for PenSoft® Payroll Solutions

VOLUME 28 • ISSUE 2
Summer 2019

INSIDE...

Internal Wage and Hour Audit

PenSoft's relationship with the Department of Labor allows us to keep customers informed on compliance issues as well as voice concerns on burdensome regulations. Most recently we spoke to an Investigator for Wage & Hour Division (WHD) of the U.S. Department of Labor, and she stated there was an increase in the number of wage and hour claims filed against employers in 2018. In fact, the WHD in fiscal year 2018, collected on average $835,000 in back wages for workers per day. See **www.dol.gov/whd/data/**

The WHD of the U.S. Department of Labor's mission is to promote and achieve compliance with labor standards to protect and enhance the welfare of the nation's workforce. The federal Fair Labor Standards Act (FLSA) governs employee pay with the purpose of ensuring: (1) all covered employees must be paid at least minimum wage for all hours worked, and (2) all covered employees must receive time and one-half of their regular pay rate for all hours worked over 40 in a week. Even though the rules seem straight forward, the complexity of adjacent labor laws makes it one of the most difficult and regularly violated areas of employment law but there are processes you can put in place to reduce the potential for violations.

How to Prepare for a Wage & Hour Audit

Now is a good time to manage your company's risk by conducting an internal audit on employee pay. An internal audit can bring to light areas of non-compliance in need of correction and provide a solid foundation for a "good-faith" defense when audited. Where to start can be challenging so here are a few recommendations from our representative for conducting an internal audit.

Internal wage and hour audits are unique for

*See **Audit** page 4*

Computer & Online Security

Computer and online technology are powerful tools for small businesses. It levels the playing field in reaching new markets, increasing sales, and productivity. However, there is danger lurking around every corner in e-mail correspondences, online threats, and criminals impersonating legitimate companies we do business with daily. The threat status has been a constant state of red for years so businesses must take an active role to protect their customers, employees and assets.

10 Tips to Help Prevent Cyber Criminal Attacks

The following ten recommendations will help in reducing the chance of your company becoming a victim of a cyber criminal.

1. Employees can be one of the biggest risks for exposing company information in part because they have not been properly trained on the company's security principles. Companies that train employees on the basic security practices and policies have a lower percentage rate of unauthorized access. Requiring strong passwords and establishing acceptable internet usage policies provides guidance for employee behavior and outlining the consequences of inappropriate behavior helps to protect the employees, customers and company assets.
2. Clean desk and computer policies ward off cyber attacks. Keeping desks clean of post-it notes containing "encrypted" sensitive information, business use only computers, and requiring all systems be up-to-date with security/virus software updates are the great defenses against attacks.
3. Firewall security for all systems regardless if they are connected or not connected to the internet helps in preventing unauthorized access. Many companies require certain computers not be constantly connected to the internet, believing they are protected from unauthorized access but that may not be the case. With so many software

*See **Security** page 2*

In observance of Independence Day, PenSoft will be closed Thursday, July 4th.

In observance of Labor Day, PenSoft will be closed Monday, September 2nd.

PenSoft® PAYROLL SOLUTIONS
PenSoft
151 Enterprise Drive
Newport News, Virginia 23603
P 757.873.2976
F 757.873.1733
info@pensoft.com
support@pensoft.com
www.pensoft.com

President's Corner

Leroy Newman
President & CEO

Incorporated on January 3, 1990 PenSoft is nearly halfway through its 30th year in the payroll software business. We began with 2 "XT" computers for programming and producing a very limited payroll software product on 5¼" floppy discs for distribution. We had a single line telephone and a one person office. It is amazing how far the industry has advanced since then.

There have certainly been challenges along the way but it's been a successful journey for PenSoft while navigating myriad payroll changes. The first really big challenge was in 1991 when the IRS separated the Social Security and Medicare taxes. This change rippled through the entire program from data input to reporting. Since then there have been many challenges (opportunities to excel) all met and accomplished by our professional staff. PenSoft and its products and services grew to its current capacity of supporting customers in all 50 States.

Currently we are in the process of preparing 2020 PenSoft Payroll for distribution nationwide on December 16, 2019. We are proud of being the payroll solution for our customers and look forward to continuing this business relationship for years to come.

APA Congress

The American Payroll Association (APA) held its annual Congress the week of May 13th in Long Beach, California. Two Certified Payroll Professionals (CPPs) from PenSoft attended the event: Stephanie Salavejus, Vice President & COO, and Melinee' Cody, Director of Support and Training.

Stephanie Salavejus, APA Vice President, Board of Directors, presented four sessions at Congress: (1) "DOL Investigation: How Would You Stack Up?", (2) "Combating Fraudulent Authorizations", (3) "The Psychology of Change Management: More Than Simply Communicating the Change", and (4) "Payroll Fraud: Detect, Deter, Defend".

Melineé Cody, CPP, was selected by the APA to serve on their Board of Advisors. Her two-year term began at the APA annual Congress on May 14, 2019. Her role is liaison to APA's affiliated local chapters located in one of nine regions within the U.S. She will work with chapters spanning from North Carolina to Florida to bring forth ideas for future APA endeavors.

Melineé is an active member of the American Payroll Association (APA) and has held her CPP Certification since 2000. She currently serves on multiple APA committees such as the Education Grant Committee, Board Leadership committee, APA Hotline, Chapter Mentor Program-CHAMPS, Certification Advisory Group, and Government Relations Task Force - Federal Tax Forms and Publication, and Unemployment subcommittees. She also received the APA Meritorious Service Award in 2012. Well done Melineé.

Congratulations

Wendy Gay, CPP, Program Consultant, recently sat for and successfully passed PenSoft's Program Consultant Level 3 exam. Her professionalism and desire to excel were the basis of her preparation for this very demanding exam. Her dedication to PenSoft and support for our customers is beyond reproach. Congratulations Wendy on your promotion to Level 3.

The Colonial Capital Chapter of the APA appointed Wendy their educational coordinator. Her responsibilities include the development, coordination, and management of certification study groups. She works closely with the Chapter board planning, organizing, and implementing educational services for the chapter's payroll professionals. This past spring she served as the instructor for the Spring APA Certification Study Group. Preparation for the fall study group is underway with the first class beginning July 8th. Thanks Wendy for a job well done.

Security, continued from page 1

vendors only offering download options there will be a time when the computer is vulnerable to viruses or unauthorized access. Connecting to the internet even for a short period of time can result in disaster and the use of flash drives to update software is not an iron-clad solution for protecting the system.

4. Security policies need to be in place and enforced. Mobile devices create a major security risk and the opportunity for unauthorized persons to access sensitive data on the device or gain access if connected to the network. Requiring all devices be password protected, data transmission security encrypted, and updates current help in protecting the employee and the company.
5. Backup, backup and backup again. Regularly backup the data on all computers and any data stored on external devices. Automating the backup process helps in ensuring the company data is protected in the event of a disaster and routinely testing the restoration of data is recommended.
6. Control both physical and remote access to company computers. Laptops are easy targets so ensure employees are trained on the company policies as it relates to all mobile devices. Keeping all devices secured during transport and at home is important.

See **Security,** *page 3*

Q&A

Q. We paid a sign-on bonus of $750,000 in February. The bonus was taxed at the 22% supplemental tax rate. The employee earned a second quarter bonus of $350,000. The total bonus amount exceeds a million dollars. Where can I locate information to explain that both bonuses are considered when calculating the federal withholding for the second quarter?

A. The one million dollar supplemental wage threshold is for the year. Your understanding of the method for calculating the withholding agrees with the instructions in Publication 15. The amount up to one million can be taxed at the 22% supplemental flat rate and the amount exceeding one million must be taxed at the supplemental flat rate of 37%.

Q. One of our executives has submitted a request for a fixed percentage to be withheld from all wages earned. When I explained the fixed percentage method is used for supplemental payments and not for their semi-weekly pay, they asked why. What can I provide to explain I cannot honor their request?

A. Print the 2019 Form W-4 instructions and highlight the section that clarifies for regular wages a flat percentage of withholding is not allowed and that a flat dollar amount is allowed only in addition to a prescribed withholding tax method. If the employee provides a Form W-4 with 24% in the additional withholding column, the alteration to the W-4 makes it invalid.

Q. Using our employee self-service portal an employee submitted an updated Form W-4 over the weekend. On Monday the payroll team completed the payroll process first before addressing any employees' requests for change. The employee filed a complaint that payroll is in error and requested their paycheck be reprocessed with the new withholding allowance. How can I explain to our CEO payroll is in complaince with withholding based on the Form W-4 we had on record?

A. Assuming the company does not have a formal policy regarding requests for withholding changes, IRS regulations can be found in the IRS Publication 15 Circular E, Employer's Tax Guide. On page 20, Section 9 "effective data of W-4" outlines a revised Form W-4 must be put in effect no later than the start of the first payroll period ending on or after the 30th day from the date it was received.

Q. A former employee paid the social security and medicare taxesav due for their group-term life insurance over $50,000 with their income tax return. I need to adjust the Form 941 to back out the employee's share of the taxes. How do I do this in PenSoft Payroll

A. Per the IRS Publication 15-B instructions, include all social security and Medicare taxes for the coverage on Form 941, lines 5a and 5c then back out the amount of the employee share of these taxes as a negative adjustment on Form 941, line 9. Generate the Form 941 for the quarter, click Setup button. Click Adjustments tab and enter in the amount for line 9 and the effective date for the adjustment.

Security, continued from page 2

7. Know who has access and secure use of all Wi-Fi networks. If your company needs Wi-Fi for guests, have separate Wi-Fi access for employees and guests and always password protect.
8. Outside access policies must be in place. Scrutinize the authorization and authentication of employees and devices wanting access to your network from outside of the company. It is important to restrict access to mission-critical employees and to constantly monitor activity from outside connections.
9. Incorporate backend protection to limit access to data and information. It is extremely rare for all employees to need access to all data systems and those who are authorized access should have a limited scope based on their job responsibilities. The policies should include reports to key personnel when unauthorized access is attempted and all incidents should be followed up on to ensure credentials have not been compromised.
10. Strong password protocols are essential. As threats increase, companies are requiring multi-factor authentication and a requirement for scheduled password changes. While it may seem cumbersome, multifactor authentication is mainstream and part of our daily lives. An authenticator solution that provides a unique pin every 30 seconds is worth the extra effort to avoid becoming a victim of a cyber criminal.

Listen to a discussion with Paul MacDonald, Director of Information Systems at PenSoft, regarding computer security and the steps needed to protect against the threats that are surrounding us.

Register and Listen! **https://register.gotowebinar.com/recording/3016859095307343105**

Audit, continued from page 1

each company, but it is recommended the audit process involves coordinating with legal counsel to review documentation relating to employee pay, including job descriptions, payroll records, and leave policies. Interviews with Human Resource personnel and executive management are needed to obtain a clear understanding of employee pay structures and employee classifications. The goal is to complete a comprehensive review of employee pay and payroll policies to identify any possible wage and hour vulnerabilities or violations.

- Employee classifications - The Internal Revenue Service (IRS) estimates up to 20% of workers are misclassified. In the report a percentage of the misclassifications are unintentional due to lack of understanding of the laws regarding worker classification, but there continues to be a considerable percentage of misclassifications being done deliberately to gain an unfair competitive advantage by reducing labor costs and avoiding paying state and federal payroll taxes. During an internal audit carefully exam all exempt employees and their job duties to ensure they are properly classified. Specifically, look beyond the job description and analyze what primary tasks and responsibilities the exempt employees are performing on a day-to-day basis.
- Overtime and Regular Rate of Pay (RRP) – Overtime pay and RRP is a common FLSA violation. The Government Accountability Office reports 95 percent of all lawsuits filed against employers include allegations of overtime violations. During the audit take a close look at your overtime and regular rate of pay calculations. What seems straight forward can become very complicated due to the lack of clarity in the rules related to employment perks, benefits and other miscellaneous items such as nondiscretionary bonuses that are required to be included in the regular rate. The level of complexity increases if the employee has multiple pay rates, piece rates or commissions. The audit process should include validating the calculation to ensure all employees are being paid in accordance to the DOL regulations. The DOL has a great resource to help employers navigate these regulations at **www.dol.gov/whd/flsa/**.
- Timekeeping policies – A timeclock systems fault is not a strong defense. As a part of the internal audit take a close look at your timekeeping policies and procedures. Here at PenSoft we require all employees to track hours worked and to sign off and verify their timesheets each pay period to attest to the accuracy of the hours being submitted to payroll. Validate the timeclock systems are correctly tracking breaks and meal periods to minimize underpayment of hours worked. While employers regularly report employees do not properly record hours worked on their timesheets, it is the employer's responsibility to ensure all hours worked are compensated in accordance to the FLSA. There are options for disciplining employees who do not take responsibility for correctly recording time worked other than not paying them. Failure to properly pay employees opens the door to a potential investigation by the DOL.
- Independent Contractors – All workers classified as independent contractors should be carefully reviewed to ensure they meet the IRS requirements. The general rule is that an individual is an independent contractor if the payer has the right to control or direct only the result of the work and not what will be done and how it will be done. Facts that provide evidence of the degree of control and independence fall into three categories under the Common Law Rule. Review any contractual agreements with your Independent Contractors, paying close attention to the degree of control you have over the contractor's activities.

The IRS website provides good resource guides for classification determination and in the event you are still unsure, request the IRS review the facts and circumstances by submitting a completed Form SS-8, Determination of Worker Status for Purposes of Federal Employment Taxes and Income Tax Withholding. Go to **www.irs.gov/businesses/small-businesses-self-employed/independent-contractor-self-employed-or-employee** for more information on correctly determining employees vs contractors.

The benefits of conducting an internal wage and hour audit far exceed the cost. Getting out in front of any violations helps in establishing a "good faith" defense.

In the event your company is selected for audit, the Wage and Hour Division (WHD) conducts virtually its entire litigation "discovery" through record audits and on-site inspections. Risks can be mitigated with advance planning and inexpensive corrective measures.

Preparation is now more important than ever before because the DOL has stated they are diligently enforcing compliance.

Leroy Newman
President & CEO

Stephanie Salavejus, CPP
Vice President & COO

Melineé Cody, CPP
Director of Support & Training

Heidi Heretick
Director of Sales & Marketing

Paul MacDonald, MCSE
Director of Information Systems

Contributing Writers
Program Support Department
Information Systems Department

PenSoft
151 Enterprise Drive
Newport News, VA 23603

Info: 757-873-2976
Support: 757-873-1199
Fax: 757-873-1733

info@pensoft.com
support@pensoft.com
www.pensoft.com

Published 4 times a year.

Articles published in this newsletter are intended as general guidelines. PenSoft shall not be liable to any person or entity with respect to any liability, loss, or damage caused or alleged to be caused directly or indirectly by this publication.