PenSoft® NEWS

Quarterly Newsletter for PenSoft® Payroll Solutions

VOLUME 23 • ISSUE 1
Spring 2014

INSIDE...

In observance of Memorial Day, PenSoft will be closed Monday, May 26th.

PenSoft® BUSINESS 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

Data Protection Through Prevention

Data protection is more than just firewalls, anti-virus software and passwords. These things keep the obvious risks minimal, but what about unforeseen and often seemingly small dangers? These unplanned surprises can potentially cause the greatest harm to what appeared to be a fully protected system. In most cases, a simple backup can prevent a company from losing valuable data.

Backing Up Can Prevent Your Company From Losing Data. What Solutions are Available?

Backups

A data backup is one of the most comprehensive protection methods and often one of the least expensive. Depending on the type of technology used and the extent of the Backup, all companies should be able to afford at least basic protection. For some, it can be as simple as pushing files onto a removable storage device. Other companies with more extensive business operations will most likely need a backup plan with more control, planning and storage space. With advancements today, options such as cloud-based storage can be very useful. Placing data on the cloud can be accomplished using a variety of web based Application Programming Interfaces (API's). Examples include a desktop, gateway or web based storage application.

Once a choice of backup is selected, the next step is determining not how much to back up, but how much a company can afford to lose. Businesses providing a majority of web based services will want to make sure their website data is protected. Service providers should exercise the highest regard for their client databases including contact, purchase history, and general interest information. Multiple copies should be kept, ideally using multiple backup methods to ensure greater security.

Finally, if the unexpected should happen, the ability to retrieve the backup quickly and easily is equally important. For companies performing services, especially on the web, how long can the business afford to be down? Every non-functional hour can

See **Data Protection,** *page 4*

PenSoft Customer Security

Would you like to put this on your credit card you have on file with us? This is not a question you will hear at PenSoft when you call to place an order. PenSoft has many policies and procedures in place to protect you and your data.

Where and how do we protect your data?

How Does PenSoft Protect Your Credit Card, Check or ACH Information?

Sales & Administration

When you call you will be requested to provide your name along with your customer number. The representative will verify you are a contact listed on the account prior to giving out any information regarding the account.

Making a purchase with us over the phone with a credit card? No credit card information is saved in our customer database or credit card processing service. Once a card has been processed we are unable to retrieve your number.

We eliminate credit card information sent to us through fax or mail. We punch out any personally identifiable information on an order form: credit card number, security code, and expiration date.

Paying with a check? After we process the payment, your check is held in a secure location and destroyed after 90 days.

See **Security,** *page 4*

President's Corner

Leroy Newman
President & CEO

This has been a hard winter with major storms across our country. We hope you and your families have been able to weather the storms without major consequences. For the safety of our employees, PenSoft closed early one day and stayed closed the next day due to a snow storm in our area. Fortunately this snow storm hit us after our peak Program Support season. We apologize for any inconvenience our closing caused you and your company.

Customer Privacy

We have all heard the horror stories resulting from the security breaches at major retailers lately. Rest assured PenSoft is doing everything possible to protect your information privacy. See the article in this newsletter describing our internal procedures to keep your information safe.

Data Protection

PenSoft is committed to protecting the privacy of your company information. We secure your credit card information from the point of sale whether you are placing an order online, faxing or calling it in to our Sales and Administrative Staff. We also secure all payroll data provided to our Program Support Consultants when they are offering support. See the headline article in this newsletter for more details.

2014 PenSoft Payroll

2014 PenSoft Payroll was released on schedule on December 16, 2013 in spite of the delayed IRS and State tax releases. As usual there were additional State tax updates after our release date. They were handled on a case by case basis and affected customers received the updates.

This was another one of our smoothest software conversion years. Due to our extensive software testing procedures, there were no major software problems. Most of the program support calls were to help customers install 2014, run W-2s from 2013, and resolve data errors. All in all it was a very good conversion.

We are researching tax changes throughout the U. S. so we can prepare the 1st Quarter update for distribution the 3rd week of March.

2013 and 2014

PenSoft ended 2013 on a high note showing growth over the previous year and thanks to our customers we are looking forward to a very good 2014.

Additional Products/Services

Be sure you are getting the most value from PenSoft Payroll by exploring the additional products and services we offer to enhance your experience. Using direct deposit, electronic pay stubs, and time online are a few ways to increase your payroll efficiency.

Protecting Corporate Identity From Theft

Identity theft is devastating both financially and psychologically for the victim. Reports of identity theft have been front page news for many years but individuals are no longer the only target. Criminals are now turning their attention to businesses to turn a profit, often resulting in a negative reputation and financial ruin for the business. For this reason it is extremely important for businesses to understand the type of information criminals target and how to reduce the possibility of becoming a victim of corporate identity theft.

Businesses are easy targets because much of their information can be easily located on the internet. Criminals will search the internet for businesses public profiles and "dumpster dive" to collect valuable information to use for committing fraudulent acts. It only takes a few key pieces of information to impersonate a business then criminals can take advantage of the business' bank accounts, credit limits and good credit ratings.

Data in need of protection:

- Federal Employer Identification Number (FEIN)
- Financial account information
- Creditor account information

Federal Employer Identification Number

Business' Federal Employer Identification Number (FEIN) is the company's identity. The FEIN is on all tax returns, financial accounts and credit applications but that does not mean it should be made readily available to anyone.

Businesses will get requests from vendors for the Taxpayer Identification Number and Certification, Form W-9. The purpose of Form W-9 is to provide your vendor with the information needed to file required tax information reports at the end of the year. Form W-9 also provides certification from the payee that the taxpayer identification number provided is correct and that the payee is not subject to, or is exempt from backup withholding.

When a request for a Form W-9 is received, have the accounting department verify the vendor is someone you do business with and is entitled to receive this information.

All too often businesses will post their Form W-9 on their websites for the public to download. This is providing valuable

See **Theft**, *page 3*

Theft, continued from page 2

information to identity thieves and brings them one step closer to successfully impersonating your company.

Financial Account Information

Financial account information is extremely valuable to identity thieves. Once they have the bank account and routing number, all they need is a signature to generate a check on your company's account. The reality is, it is almost impossible to keep this information secure especially if you process check payments for accounts payable or payroll. To reduce the probability of identity thieves getting your financial account information, talk to your bank about direct deposit for paying your employees. Use Automated Clearing House (ACH) direct debit to pay your vendors with an ACH filter on the account.

An ACH filter prevents unauthorized payments to "fake" vendors. Many banks automate the process and when an ACH item exception is received, the business is sent an e-mail notification requesting the authorized contact to confirm if the payment should be processed.

Using an ACH filter ensures only approved ACH transactions post to their respective accounts and your company has reduced risk for payment fraud.

For many businesses checks are the preferred method to pay employees and vendors. Businesses should to talk to their bank manager about options available to protect unauthorized transactions. Positive pay service is an option many banks offer.

Positive pay is a service where the business, prior to distributing check payments, provides the bank with a payment file. The payment file contains the information on checks processed for payment and the bank will match the checks being processed with the information on the file. If a check is presented that is not on the file then the bank will call the business for instructions or deny the payment request.

Creditor Account Information

Every business has filled out a credit application to obtain credit with a vendor. Identity thieves use a business' creditor information to impersonate the company and obtain credit for their fraudulent activities.

Creditor account information should be stored securely or destroyed if no longer needed. Document destruction services are readily available and will protect the privacy and confidentiality of your business information.

Avoid your organization becoming a victim of identity theft by proactively protecting important information. The risks go far beyond the loss of money and regulatory compliance.

Corporate identity theft undermines your organization's financial stability, reputation, credibility with customers and creditors and the trust of your employees.

Q&A

Q. My state unemployment tax rate changed. Where can I apply this in PenSoft Payroll.

A. To change the rate:

- Click Company on the toolbar.
- Highlight the desired company.
- Click Modify.
- Click State Setup.
- Change the rate for the appropriate quarter(s).
- Click OK to save the changes.

Q. Is PenSoft Payroll compatible with Windows 8?

A. Yes. PenSoft Payroll can be installed and run on the following operating systems: Windows XP, Windows Vista, Windows 7, and Windows 8.

Q. Where can I add an additional account number to my general ledger report for a new income I created?

A. To add a new account number to the setup of the general ledger report:

- Click Reports on the toolbar.
- Click Pay Date Reports.
- Click Report Setup under General Ledger.
- Ensure "Include payroll data in the report" box is checked.
- Click Setup Accounts.
- Click into the box for the new income you created.
- Enter the account number of the new income.
- Click OK to save.
- Click OK to exit setup.

Data Protection, continued from page 1

be a detriment to the very livelihood of the company. If choosing a backup method in-house such as a server or tape system, ensure the holder of this data can be available on short notice. If a third party organization is responsible, check their service record and ask for references. Request a backup system with the ability to be restored quickly and check their service hours to determine what the longest possible window of downtime the company may have to endure.

Backups & PenSoft Payroll

PenSoft provides a highly effective way to protect payroll data created within the software. Be it a computer, server, or removable storage device, PenSoft backups contain only data. They are not encumbered with the software package as well, as PenSoft allows registered users to download the software from the website at any time with their login. *This allows for smaller more compact backup files to store.* Once the program is downloaded and installed, restoring data is as simple as a few clicks of the mouse, providing peace of mind in even the most difficult situations. Trust PenSoft for all your payroll needs, and rest easy knowing your data is easily protected.

Security, continued from page 1

Website

All orders placed online are secured via SSL 2048-bit version SSL certificate. This encryption offers strong data encryption between our clients and our web server. Credit card numbers are not saved and are not retrievable by PenSoft employees.

Program Support

When you call Program Support you will be requested to verify certain account information prior to a Program Consultant assisting you.

Sending in a backup for assistance? Once Program Support has completed their evaluation of your data, it is deleted.

Webservice Contracts & ACH Billing

All webservice contracts are held in a secure location. Access to ACH information is restricted to a limited number of employees and the ACH billing is restricted to only specific individuals who process the billing.

We take the precautions above to reduce the chances of our customers having their personal payment information from being compromised. PenSoft is dedicated to protecting your data in-house. Ensure you secure your client data also. See Data Protection Through Prevention on page 1.

2014 Training Opportunities

Quarterly Reconciliation Webinar

Earn one RCH by attending our popular quarterly Reconciliation webinar. The 60 minute live webinar $99 per phone connection. The one hour webinar is at 2:00 pm Eastern time on the following dates:

- March 20
- March 25
- March 27
- April 1
- April 3
- April 8
- April 10

Quarterly Training at PenSoft

Looking to get more out of PenSoft Payroll? Consider taking a training course at PenSoft to increase your productivity and gain new skills!

Download a brochure at **www.pensoft.com/document/PenSoft_Payroll_Training_Brochure.pdf** and check it out!

- March 10-11
- June 9-10
- September 8-9
- December 8-9

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.