Version 7.4 & higher is Critical for all Customers Processing Credit Cards!

Data Pro Accounting Software met the latest credit card processing requirements with its release of **Version 7.4** due to the recently mandated requirements by the credit card industry. This version release, and all future version releases, incorporates all of the new mandatory features required by the **Payment Card Industry**.

This is a critical issue that any business owner must address if their firm is **processing credit cards**. The **Payment Card Industry** has created a special security standards council for the purpose of protecting consumers from card data theft and fraud. To this end, new standards have been imposed on every level within the industry from merchants, banks, processors, hardware and software developers, and point of sale vendors.

The new standards for protecting card data is called the **"Payment Card Industry Data Security Standard"** which sets all guidelines for how cardholder data is secured, stored, processed or transmitted by merchants and other organizations. The **"standard"** is managed by the **PCI Security Standards Council (PCI SSC)** and its founders: **American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.**

What does this mean to you as a business owner?

A lot! It means that **virtually all liability is now passed down to you as the merchant!**

It means that between Data Pro Accounting Software, as your software provider, and you as **" the merchant,"** the responsibility for the security of credit card data has now been delegated between the two of **"us."** We are informing you that we have done our part to assist you in protecting this process. In other words, it requires that you be responsible for insuring that you comply with the **PCI-DSS** requirements, one of which requires that you use a payment application that is **"PA-DSS compliant**."

By using **Data Pro's Infinity POWER** products ***(Version 7.4 & higher)*** in conjunction with the **DP/CHARGE Payment Server**, you are utilizing a **"PA-DSS compliant software solution"** for your business.

None of our other previous product integrations or earlier software versions have gone through **PA-DSS** compliance. **Only product releases *(Version 7.4 & higher)* fully comply with the PA-DSS requirements!**

Even if you are processing credit cards using stand-alone credit card terminals, you still have obligations to become **PCI-DSS** compliant, even though you are not processing your credit card transactions through the Data Pro's **Infinity POWER** software applications.

Risk levels have never been higher for handling credit card information. Hackers want to steal and employees can tend to mismanage your customer's credit card information. Either way, ultimately **YOUR COMPANY** will be the one who gets held liable if damages occur. Failure to abide by these standards can result in fines from the Card Associations, especially in the event of a security breach. You can hardly turn off the news these days without seeing that major companies too are constantly having their systems breached. Therefore, any size of company can become vulnerable without the proper steps being taken.

Banks and credit card processors over the years have ascertained that some of the biggest breaches in credit card data have occurred by unsuspecting merchants who have allowed smart people *(often from foreign countries)* to hack their networks and capture large quantities of credit card numbers which has left them liable for replacing the money stolen from those cards.

Therefore, the shift is on in the card processing industry to make those responsible for those security breaches fully liable instead of those higher up in the card processing cycle. This is the equivalent to a **"Y2K shift"** in programming requirements for virtually every software company who touches credit cards.

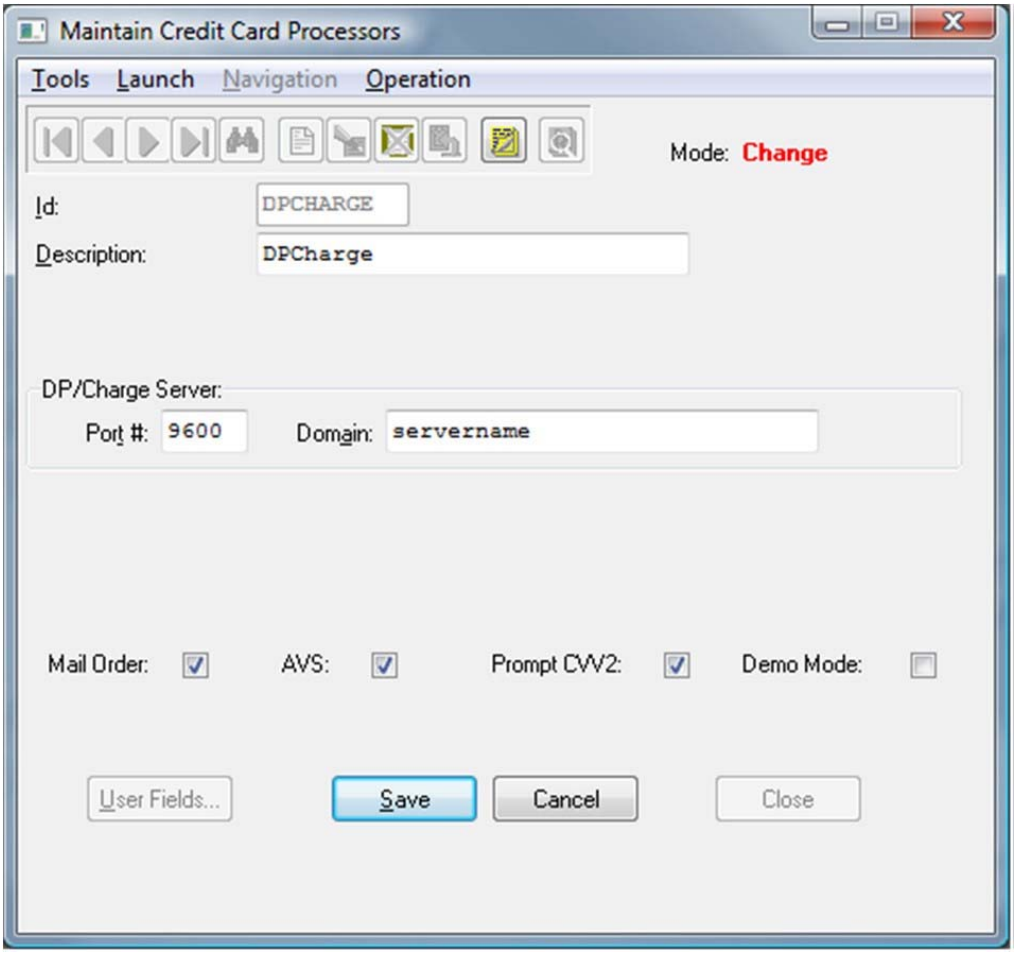
Many companies have credit card processing features imbedded throughout many software modules and options. The result is that as a software company we have to spend tens of thousands of dollars to become **"compliant"** and ultimately **"validated"** by the industry.

Further, any future changes you make to your software may require another round of **"certifications"** and **"validations"** each time you upgrade your software. Data Pro Accounting Software, Inc. has done this.

How will this affect current Data Pro Customers?

With the release of software products ***(Version 7.4 & higher)***, Data Pro's **Infinity POWER** accounting software products are what are termed **"PA-DSS Compliant."** As a Data Pro customer paying a current Annual License Fee **(ALF)**, you are automatically entitled to the upgrade to **Version 7.4, or higher,** at no additional charge.

This means that all software functionality inside the specific accounting modules that deal with credit card processing have already been specifically upgraded to deal with the new mandates.



This is the new set up option in Accounts Receivable for Maintaining Credit Card Processors.

This includes the ***Accounts Receivable, Point of Sale, Sales Order Entry, DP/STORE, and DP/DashBoard*** modules. That will get you most of the way to becoming compliant. However, there are a few more steps now required to get fully compliant.

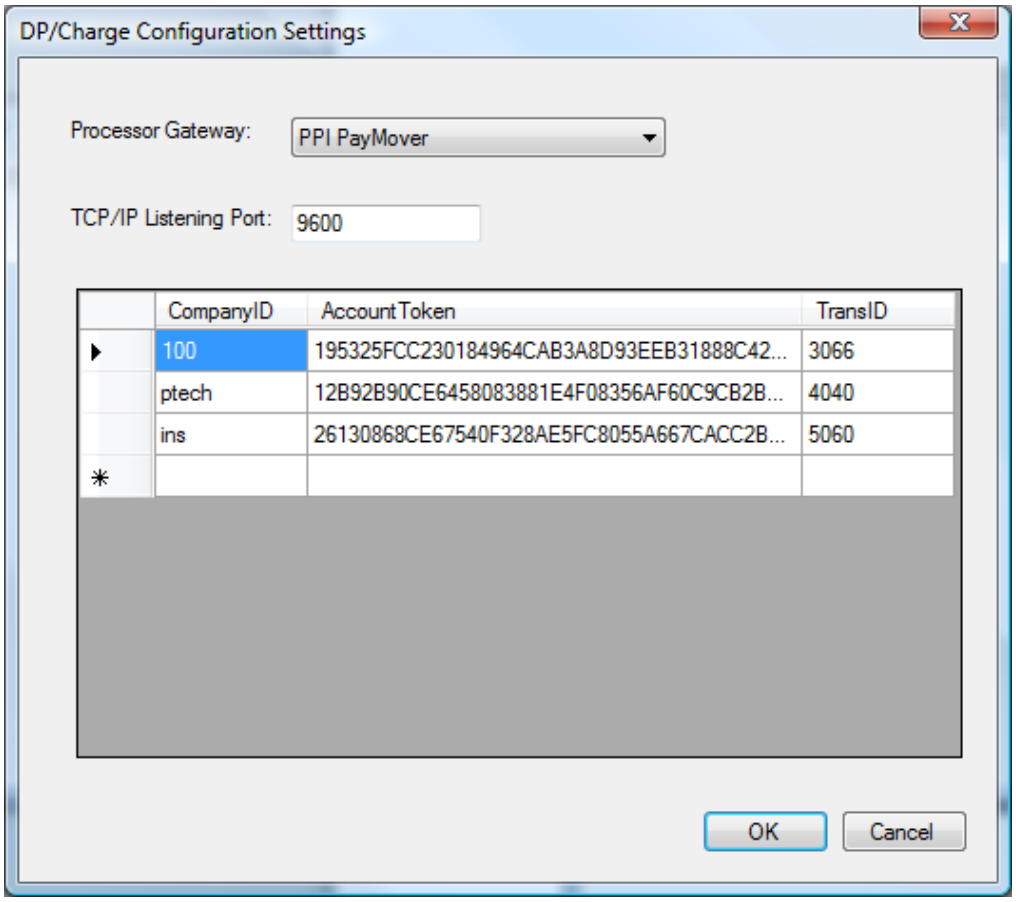
DP/CHARGE

One of the primary concerns of the Data Security Standards is the protection of cardholder data. Version 7.4 & higher uses a specific system that stores cardholder data **"off-site"** in a secure data vault at **OpenEdge** and allows access to this data using a highly encrypted **"tokenization"** system with the remaining data in your **Infinity POWER** software applications.

This is all made possible due to a new and **"secure"** credit card processing module called **"DP/CHARGE."**

Regardless of what you have been using to access your credit processor up to this point, including the direct access options inside **Infinity POWER's Accounts Receivable** or any of the current versions of third party programs such as **"IC/Verify and PC-Charge,"** ***they are not PCI-DSS compliant!*** None of these options have been through the certification process with Data Pro.

One of the mandates of becoming **PCI-DSS** compliant is to remove any database that specifically contains a database of credit card numbers from your internal network.



DP/Charge's configuration stores access to all Merchant ID information on the OpenEdge Token Vault using the OpenEdge Point-2-Point encryption technology which monitors all transactions using a separate Transaction ID by company.

Designed to support **"Multi-Companies"** and **"Unlimited Users," DP/CHARGE** acts as your real time gateway to the integrated credit card processor we have selected. **OpenEdge** was chosen as our primary credit card processor at this time because of their industry leading awareness of the **PCI-DSS** standards and their representation on the **Security Standards Council** itself.

To become compliant, many firms have developed features that meet the minimum thresholds for the current deadline. That is not the way **OpenEdge** operates, nor allows their development partners to focus their development standards. They have gone significantly further into the future and that future is **NOW!** To become a **OpenEdge** marketing partner, everything Data Pro Accounting Software did in its development of **DP/CHARGE** and **Version 7.4 & higher** was to become **"PA-DSS compliant"** and ultimately **"validated"** by the **Security Standards Council**.

Coming soon, the **OpenEdge EMV Solution** will be available within all of the **Infinity POWER** and **Infinity Commerce** applications.

This fraud-reduction technology protects card issuers, merchants and consumers from losses due to the use of counterfeit and stolen payment cards at the point-of-sale. **EMV Smart Cards** are embedded with a chip that interacts with a merchant's POS device, ensuring the card is authentic. This chip technology is virtually impossible to duplicate.

To illustrate why, according to industry security expert PCI-Assure, "92% of card data compromises take place in small businesses with low processing volume."

Validating software companies to ensure that they are **PA-DSS** compliant is only half the process. If there is a breach, the first place the Secret Service will look is at the software you are using to verify that the merchant is in fact **PCI-DSS** compliant all the way down to the specific version of software you are running. In Data Pro's case, any version lower than **Version 7.4** is **NOT PA-DSS compliant**.

Data Pro Customers who have not become **"Validated"** haven't understood their level of risk yet and won't until they are **"breached"** and fined for the damages caused by the culprits capable of stealing card data. All merchants who process credit cards are required to comply with **PCI-DSS**, which includes completing the Self-Assessment Questionnaire **(SAQ)**. The **SAQ** is a validation tool used to assist merchants with meeting their **PCI-DSS** compliance requirements.

On the Data Pro web site, you will find a link that will allow you to print out this **"Self-Assessment Questionnaire."** Remember, you can complete this form completely on your own without any further expense on your part other than the time and effort required for your own internal review. However, many merchants find this an uncomfortable process and aren't sure how to answer the questionnaire and aren't clear whether they have in fact met the requirements appropriately.

That is why the industry has **"Qualified Security Assessor"** organizations that can assist in this process. By partnering with **OpenEdge**, Data Pro made sure we had a process in place that would allow us to guide our merchants through this process with minimal confusion and expense.

OpenEdge recognizes the obstacles merchants face in meeting **PCI-DSS** compliance requirements. To help you with this endeavor, **OpenEdge** has partnered with **PCI-Assure**, a leading Qualified Security Assessor **(QSA)** and Approved Scanning Vendor **(ASV)**, to offer you **OpenEdge** PCI Validation**.** It's a comprehensive service that offers a PCI compliance program tailored to how you run your business featuring the **OpenEdge** PCI Breach Reimbursement Guarantee!

For businesses with integrated IP-based payment processing, the program features a full-featured PCI compliance portal with easy-to- use navigation and award-winning vulnerability detection.

Featuring PCI-Assure® PCI Manager, the program includes:

- PCI compliance portal featuring the **PCI Wizard** and **To Do List** to help determine the steps required for your business type, making the process easy to complete and informative.
- Vulnerability scanning service for up to **3 IPs** to help determine the vulnerabilities in your network.
- On demand external scanning – ad-hoc scans up to **12** a year.
- The **Security Policy Advisor** for assistance with **PCI DSS** policy documents and requirements – one per merchant ID **(MID)** – and to develop your own unique internal best practices.
- The **PCI-Assure Agent** for up to **3** devices for simplifying the scanning process and providing ongoing compliance monitoring for the systems the agent is installed upon.
- Access to the **PCI Video Assistant**, on-line help test, tutorials and educational tools for your staff ***(up to 10 users)***.
- Immediate user access to web-based scan report results upon scan completion.
- **24/7** phone and email support from **PCI-Assure** for **PCI DSS** questions.
- Electronic report submission of quarterly **PCI** compliance letter **(executive report)** to **Acquirer**.
- Annual cost of **$149** for one **MID** up to **3** devices **(IPs)**.

Once you achieve and maintain **PCI DSS** compliance you may be eligible to be reimbursed up to **$100,000** by **OpenEdge** for forensic reviews, fines and card reissuance costs resulting from a card data breach.

The key is this annual service will feature a scanning service to monitor network traffic on your internal network to monitor whether or not credit card data is passing across your network or not. It will also scan key databases and other locations to ensure your staff are staying in compliance and keeping your company safe and in compliance.

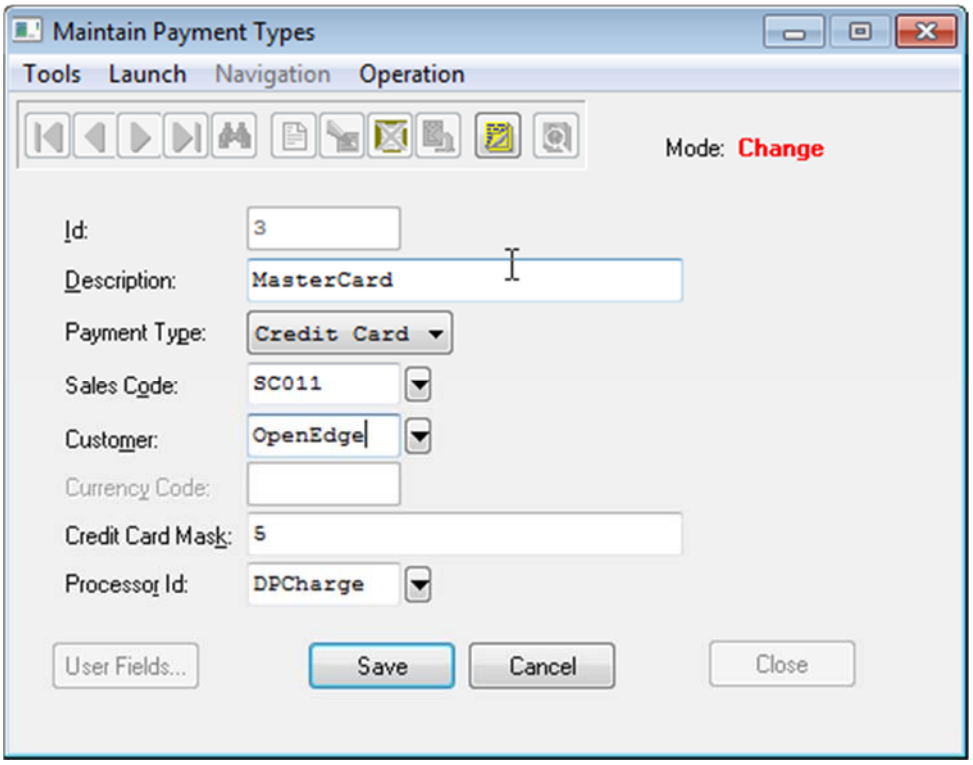
Keep in mind, however, that transmitting card data across a network is only one kind of breach of PCI compliance. How many of your staff members have Excel spreadsheets with customer's card numbers they use when asked to charge again a sale transaction in the future? Or, do they have the card number written on a **"post-it-note"** that's stuck to the side of their computer monitor? These are the classic examples of breaching the **PCI-DSS** standards.

Since your firm will be held accountable for any security breaches if this data is stolen or lost, you have to revisit whether you can afford your current non-compliant policies any further? The whole industry is re-evaluating theirs.

And, they aren't going to take any more blame, they are going to pass it down the line to the lowest common denominator which is on the software you use and the business practices you execute every day! Data Pro had to make tough choices forced on us by the credit card industry. We certainly had no interest in interrupting our client's current credit card processing practices. However, in light of all of the liability directed at both the software companies and the merchants at this point, we had to select a Credit Card Payment Processor we could utilize to protect our clients with maximum protection and one that could offer them the best possible rates on the market.

OpenEdge offers the most secure features of any Payment Processor on the market today. Further, their motto is that they will **"meet or beat"** any rate our customers are currently receiving from their current card processing firm.

Defining Your Payment Types in Infinity POWER



Defining your payment types is as simple as before!

Remember, first and foremost, that your current card processor does not necessarily mean your **"Bank."** If you are using Bank of America, Wachovia, SunTrust, Regions, Wells Fargo or any other local or national bank, you will **"continue"** to utilize them. You will simply now need a new **"Merchant ID"** from **OpenEdge** which will process your VISA, MasterCard, Discover and American Express transactions and deposit the funds generated from those transactions into the bank account you select for them. **You must have an OpenEdge Merchant ID to utilize DP/CHARGE.**

These two items, in conjunction with an upgrade to **Version 7.4 & higher** will make your firm **PCI-DSS compliant**. If you are processing with cash drawers, card swipes and receipt printers, you may upgrade your current card swipes to an **OpenEdge "encrypted card swipe"** for just **$149** each. They are connected through a USB port.

TYPICAL QUESTIONS:

What will happen to my current credit card processing options if I upgrade to Version 7.4 or higher and I don't have an OpenEdge Merchant Account or DP/CHARGE?

You will not be able to continue to process credit cards as you have done up until now. All master configuration options previously found in **Version 7.3 and lower** which supported other integrated processing solutions such as **NOVA, IC/Verify** and **PC Charge** are gone.

What if I need the latest PAYROLL changes which come out each year?

You will have to upgrade to get them and you will need to become **PCI-DSS** compliant as well. We can no longer support one without the other.

What do you have to do at this point?

1) Determine whether you process credit cards in any way or not. If not, none of this affects you. You are done!

2) Contact Data Pro Accounting Software and ask for one of our trained account managers to assist you in guiding you through the upgrade process. After we speak with you about upgrading, we will submit your information to the Account Representative at **OpenEdge** who will then contact you to establish your new Merchant Account **(ID)**. Alternatively, you can go to our web site and register on-line at **www.dpro.com/ppiregistration** and enter your company information and contact information and they will be glad to contact you directly to assist you in acquiring your **OpenEdge Merchant ID** and/or help you work through your **PCI-DSS Merchant Validation** process.

FAQs:

What is PCI-DSS?

The Payment Card Industry Data Security Standards **(PCI-DSS)** is a set of requirements for enhancing payment account data security. These standards were developed by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International to facilitate industry-wide adoption of consistent data security measures on a global basis.

Why was PCI-DSS Created?

The **PCI-DSS** requirements for security management, policies, procedures, network architecture, software design and other critical protective measures is intended to proactively protect customer account data.

I have never heard of PCI Compliance before, is this new?

No. Merchants have been advised to take the PCI Self-Assessment Questionnaire **(SAQ)** to identify potential security risks in order to achieve PCI compliance for the past **3** years. The framework of the PCI data security standards is not new and has been required in different forms for some time now and continues to evolve.

What happens if I don't get certified?

If you do not comply with the security requirements of the card associations, you put your organization at risk of payment card compromise. In the event that your business is compromised, you may be subject to fines that range from **$10,000 to $500,000** or more per incident.

You will also be liable for the cost of the required forensic investigations, fraudulent purchases, and the cost of re-issuing cards. You may also lose your credit card acceptance privileges. Various processors will impose additional fees for each month that your account has not been validated as PCI compliant or in any given month your account is deemed non-compliant. You must maintain your compliant status once it is obtained in order to prevent this fee in the future.

What does this mean to me and my business?

All entities, merchants and service providers that store, process, or transmit cardholder data must meet **PCI-DSS** requirements. Requirements for certification vary depending on the number of transactions an entity processes, and the manner in which they are processed.

What am I required to do to become PCI Compliant?

The minimum requirement for a level **4** merchant is to complete a PCI-DSS Self-Assessment Questionnaire **(SAQ)** on an annual basis and achieve a passing score. If you electronically store cardholder information or if your processing systems have any internet connectivity, a quarterly network vulnerability scan by an approved scanning vendor is also required.

Which PCI Self-Assessment Questionnaire (SAQ) do I need to complete?

The PCI Self-Assessment Questionnaire is a list of questions used to assess your compliance with the requirements of the **PCI-DSS**. In February of 2008, the PCI Security Standards Council released four versions of the questionnaire to account for different merchant environments.

1. SAQ A: Addresses requirements applicable to merchants who have outsourced all cardholder data storage, processing and transmission.
2. SAQ B: Created to address requirements pertinent to merchants who process cardholder data via imprint machines or standalone dial-up terminals only.
3. SAQ C: Constructed to focus on requirements applicable to merchants whose payment applications systems are connected to the Internet.
4. SAQ D: Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under the types addressed by SAQ A, B or C.

What is a Quarterly Network Vulnerability Scan?

A vulnerability scan is an automated, non-intrusive scan that assesses your network and Web applications from the Internet (on the external-facing IPs). The scan will identify any vulnerabilities or gaps that may allow an unauthorized or malicious user to gain access to your network and potentially compromise cardholder data. The scans provided by **PCI-Assure** will not require you to install any software on their systems, and no denial-of-service attacks will be performed.

How long is the PCI compliance certification valid?

The length a PCI compliance certificate is valid depends on whether your business requires a questionnaire or scan. If your business only requires the annual questionnaire, PCI Certification is valid for one year.

If your business requires quarterly scans, PCI Certification is valid for three months at which time your next quarterly scan will be due. If you change the manner in which you store, process or transmit cardholder data, you may increase the vulnerability of your business and must contact **PCI-Assure** or third party QSA/ASV for recertification.

What if I am required to upgrade my equipment or software to become compliant?

As part of becoming PCI compliant you may be required to upgrade your equipment and/or software to a **PCI-DSS** certified version. You must contact your equipment and/or software vendor to discuss what options may be available and the costs associated with those options, if any.

Once my business becomes PCI-DSS compliant, does that prevent a security breach from happening?

These actions help prevent security breaches but do not provide a guarantee to your business. If and when you change the manner in which you store, process or transmit cardholder data, you may increase the vulnerability of your business. Also, similar to the regularly required updates to anti-virus and firewall software, data security is also continually subject to new threats. We encourage you to stay up to date on data security requirements.

If I change the way in which my business stores, processes, or transmits cardholder data am I required to re-certify?

If you change the manner in which you store, process or transmit cardholder data, you may increase the vulnerability of your business and must contact **PCI-Assure** or your chosen third party QSA/ASV for recertification.

Is there an additional cost if I change the manner in which my business stores, processes or transmits cardholder data?

Based on how you change your processing, there may be an additional charge. To determine what, if any, additional charge may be incurred contact **OpenEdge**, **PCI-Assure** or your chosen third party QSA/ASV.

How do I sign up for an OpenEdge Merchant ID?

www.dpro.com/ppiregistration

DATA PRO ACCOUNTING SOFTWARE, INC.

Contact your Account Manager today at:

800-237-6377 or 727-803-1500 (Press 1 for Sales)

or e-mail to:

dpasales@dpro.com

Marketing Partner for:

openedge