



ICINITI Corporation develops integrated eCommerce and Payment Processing Solutions for Sage Accpac ERP

PCI-DSS Compliance

Today, Credit Card Security is a huge issue that has resulted in the credit card industry creating a set of rules for safeguarding credit card data called Payment Card Industry - Data Security Standards (PCI-DSS). These rules are fairly logical and are really things that most companies would want to do anyway.

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

In the press, the internet has borne the brunt for most of the credit card security breaches that have taken place; however most of the large credit card data losses have been through people using the internet to break into a company's network and grabbing unencrypted credit card data. They have not been from people grabbing credit card data as a person or company does a credit card transaction over the internet. For this reason, PCI compliance leans heavily on network security. As someone accepting credit cards or contemplating accepting credit cards it is not only critical that your payment application securely stores the credit cards in an encrypted format, but that your network is secure and that your passwords are strong. Newer versions of Iciniti Store force you to change the admin password and strongly suggest that it be a secure password. A secure password is one that has at least six letters, has nothing to do with your company name or phone number and that mixes upper case letters, lower case letters and numbers. Your main network, database and administrator passwords should be changed once every three months and you should not use the same password for at least a year and a half. Because of the burden put on a small company by PCI compliance some companies are opting to not accept credit cards. This is unnecessary overkill. PCI compliance is very strict when a company stores credit card information on their servers, and for obvious reasons it should be. However, credit card payment options like Sage Payments, Payment Vault or PayPal's Website Payments Standard and Pro allow companies to accept credit cards without storing any credit card data locally. This alleviates a company from having to respond to large portions of the PCI-DSS questionnaire.

In the case of Sage's Payment Vault the credit card is passed immediately through a secure gateway to the Sage Payments servers and the servers send back a "tag". If, for example, you were to send credit card number 4111111111111111 to the Sage servers they may send back the tag FGQ098372GTY. This tag is now stored in your system and represents the credit card number of your client, which is securely stored on the Sage Payments servers. If the client calls in again and says

just use the card on file you would, through Iciniti Credit Card, automatically send back to Sage Payments the amount of the purchase and tag FGQ098372GTY, and Sage's servers would find that record in their database and understand that they were to use credit card 4111111111111111 for the transaction. In this way if someone were to hack your network they would find no meaningful credit card information on your servers and even if they did steal the tag numbers they are useless unless they are sent from your location with your terminal ID and password. This method works for both internet transactions and in-house transactions through applications such as Iciniti Store and Iciniti Credit Card.

Paypal takes a slightly different route. The PayPal method is called an off-page process. When a payment is made on a web site and the customer clicks that they want to pay by credit card a new page is opened at the PayPal site and the credit card information is entered there. This means that no credit card information is being entered into your system at all. PayPal then sends a code to your site that says whether the transaction was accepted or not. You have the value of the transaction at your site and acknowledgement that the transaction was accepted from the PayPal site and the order goes into your accounting system as a pre-paid order (this works for PayPal payments too). This method only works over the internet and would not work out of your accounting system.

For more information on PCI-DSS compliance please go to [Security Standards Council](#)<

PA-DSS Compliance

Iciniti attempts, to the best of our ability, to allow our customers to make choices that suite the way that they do business. Therefore, all three methods - storing encrypted credit cards on site, Tagged transactions and PayPal off-page are supported by Iciniti Store and Iciniti Credit Card. Each one has its pros and cons; however the tagged transactions and PayPal methods will greatly reduce a company's PCI-DSS certification time and costs unless their credit card payment application is PA-DSS (Payment Application - Data Security Standard) certified.

As an industry leader in Credit Card Payments, in the Sage Accpac ERP world, Iciniti is dedicated to our client's security. Years before standards were regulated Iciniti was already utilizing 256 bit Advanced Encryption Standard (AES) encryption.

Sounds great but what does it mean. AES is a Federal Information Processing Standard (FIPS) selected by the U.S. National Institute of Standards and Technology (NIST). AES has been the official standard in encryption since 2001 and independent test by the NIST show that if you had a machine that could attempt 255 keys per second it would take 149 trillion (yes...with a T) years to crack the code and extract a credit card number. In any case most credit cards issued today will have expired by then.

In addition to the things we have done to keep credit card data secure since we introduced Iciniti Credit Card; Iciniti is now going through PA-DSS certification. This is an in-depth testing of Iciniti's web store, credit card application and order reader to ensure that they each meet the highest standards of credit card security as set by the PCI Security Standards Council.

The PA-DSS certification process not only looks at a company's encryption algorithms and encryption key security, but it delves deeply into development standards and documentation. Once certified you, our customers, will know that;

- you are using software that has met the highest standards in credit card security,
- our web store has been tested against all known types of security attacks,

- our documentation describes exactly how to install our systems in a way that will assure you are PCI compliant, and
- that Iciniti is dedicated to an ongoing testing process that will keep it that way.

For more information on PA-DSS certification please go to [PA-DSS Security Standards Council](#)