

Wisconsin Adopts Tighter Requirements for Security of Credit Card Data



Payment Card Industry Data Security Standards

We live in an electronic age where we can pay for gas by swiping a key fob, price compare dozens of airline tickets with the click of a mouse, trade stocks using our phones, and find race results online from community fundraiser runs from the past ten years. While technology creates significant conveniences for the general public, it also creates significant opportunities for criminals for identity theft, credit card fraud, and a myriad of other crimes, all without leaving the comfort and relative anonymity of their own homes.

In an effort to increase overall security of financial account data, the State of Wisconsin adopted the security provisions of the Payment Card Industry Data Security Standards (PCI/DSS). While enforcement of PCI/DSS does not begin until July 1, 2010, the standards apply now.

The key provision of PCI/DSS is that merchants are required to "certify" that they are in compliance. All merchants who accept credit or debit cards for payments are subject to the **PCI Data Security Standards**, which were set to assure the safety and security of information collected from consumers from outside theft.

Merchants will now be required to assure that customer data is secure and encrypted on any software and hardware that may have exposure to credit card data. This includes computers, software programs, and credit card interface pads such as a card swipe pad or other form of gathering credit or debit card payment information.

Every party involved with a credit or debit card transaction is considered responsible for assuring that the data is secure. This includes the merchant, the vendor that provides the merchant with credit card processing equipment, and software vendors that provided transactional and accounting programs. Failure to secure data and failure to become certified may result in fines or removal from the ability to take credit or debit as a form of payment.

History of the Payment Card Industry Data Security Standards

In an effort to increase public and business awareness of financial account data protection, the financial industry created the **Payment Card Industry Security Standards Council** in 2006. Founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., the Council is continuously developing security standards and tools for businesses to help counteract the ongoing problem of identity theft and account data breach.

Is PCI compliance a law?

While it is not currently a *federal law*, Wisconsin adopted PCI standards into law in March of 2006. There are other states with similar laws already in effect and some additional provisions that may go into effect to force components of the PCI Data Security Standard (PCI DSS). In addition, there is a big push by legislature and industry trade associations to enact a federal law around data security and breach notification.

Certification Requirements

Merchants are required to maintain the following security systems and prove through certification that the security is in place:

- Build and Maintain a Secure Network
 - ✓ Install and maintain firewall configuration to protect cardholder data
 - ✓ Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
 - ✓ Protect *stored* cardholder data
 - ✓ Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
 - ✓ Use and regularly update anti-virus software
 - ✓ Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
 - ✓ Restrict access to cardholder data by business “need-to-know”
 - ✓ Assign a unique ID to each person with computer access
 - ✓ Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
 - ✓ Track and monitor all access to network resources and cardholder data
 - ✓ Regularly test security systems and processes
- Maintain an Information Security Policy that addresses information security

New Rules at a Glance

1. Software used for the storage of credit card information must be secure and encrypted.
2. Computers and networks must contain firewalls, passwords, and be encrypted.
3. Businesses must establish policy for the safety of customer information
4. Merchants must monitor who accesses the data, and when and why the data is accessed
5. Merchants should coordinate compliance with their service providers.

Certification should be handled through the service that the merchant uses to process credit card data such as a bank or merchant services provider. Vendors will, for a fee, provide a certification questionnaire and perform a verification of all systems to check to assure all security measures are in place. The typical fee charged by the vendors is \$50 - \$300.

More information regarding PCI/DSS and the requirements may be found at:

<https://www.pcisecuritystandards.org/index.shtml>

Integration With Accounting Software

Accounting software developers have been aware of PCI/DSS and have integrated final requirements into current software versions. We recommend you integrate your accounting software compliance into your business' Information Security Policy.

Peachtree Accounting	QuickBooks Accounting	Other Accounting Software
<p>Peachtree is completely PCI compliant with their latest release of their software. The 2011 version has encryption contained within the program. If you are maintaining credit card information on your Peachtree software and keep client credit card numbers on your client forms within Peachtree, we highly recommend that you upgrade to Peachtree 2011 to assure compliance with PCI standards.</p> <p>Please refer to Peachtree Accounting's Website for information.</p>	<p>QuickBooks Pro, Premier, and Enterprise have been PCI compliant for some time. QuickBooks has had the required encryption in place that meets PCI/DSS requirements since the 2008 versions. This also holds true for companies that use the online version of QuickBooks. There is no need to do anything further with the software unless you are using a version older than 2008</p> <p>Refer to the QuickBooks Website for further information.</p>	<p>While most mainstream accounting software programs are PCI compliant, especially with their current versions, many businesses use industry specific software or potentially have offline systems in place for securing credit card data.</p> <p>Accordingly, we recommend that all businesses contact accounting software providers and look closely at their internal systems to ensure compliance.</p>

Where Do You Go From Here?

With the new certification rules going into effect, now would be a great time to give your business a check-up:

- ✓ Review your computer systems, software, and tools used to capture customer credit account information,
- ✓ Assure that you have the latest patches for your software and that your virus and firewall protection is up to date,
- ✓ Contact your service providers for your credit card processing to see what needs to be done to assure you are in compliance, and
- ✓ Finally, review your accounting software to determine if you need to upgrade your software version.

If you have questions or would like assistance with assuring that you are ready for the changes in PCI/DSS standards please feel free to call David Chermak or Kevin Smith at 414-271-3966. You can e-mail us at dchermak@komisarbrady.com or ksmith@komisarbrady.com.

Please see our publications on the Komisar Brady website for further updates and information <http://www.komisarbrady.com/resources/publications.htm>.