

# PCI is here! PCI is here!

*By John Mayleben*

While it might not be as exciting as the number of lanterns in the belfry of Boston's North Church and Paul Revere's famous pronouncement the British were coming, we have passed the deadline for level 4 merchants to have completed their PCI (data security) certification.

Level 4 merchants are those who process less than one million card transactions for each of the card brands (Visa, MasterCard, Discover, American Express).

As a level 4 merchant, you must complete a self-assessment questionnaire and confirm (attest) that you are not inappropriately storing cardholder data. You must also document that you are adhering to the 12 core principles of PCI-DSS:

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords
- Protect stored data
- Encrypt transmission of cardholder data across public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to data by business need-to-know
- Restrict physical access to data
- Assign a unique ID to each person with computer access
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security.

In addition to reviewing these 12 principles, you should take a minute and watch how your staff is handling customer transactions. A number of merchants, when pushed to review their various procedures and processes, have discovered that cardholder data are being inappropriately stored, handled or transmitted.

Usually the reasons for these outdated procedures made sense at some point in the past but now simply create an exposure for the business owner.

None of us wants a data breach. The negative impact of publicity, the cost of remediation, and the fines from the card associations are just a few of the reasons. In one case involving a

restaurant (not one of our merchants), the business owner ended up spending about \$40,000 to respond to and resolve a relatively small data breach.

Information about these 12 core principles and the different self assessment questionnaires can be found on [www.retailers.com](http://www.retailers.com) under the “forms” tab. Please make sure that you take a minute and review the process of certifying that you are PCI Compliant. Once you have done that, take time to complete the SAQ and safely store the SAQ in your files.

*Reprinted with permission of Michigan Retailers Association. John Mayleben is MRA's senior vice president, technology and product development.*