

## Payment Card Industry Standards: What Retailers Need To Know

Rules and guidelines protecting confidential customer information have long been part of the health care and financial services industries. Now, similar rules have been put into place for retailers, service providers and any other business that accepts payment cards. As in other fields, the stakes for non-compliance are high.

The payment card industry is putting the onus on merchants to protect confidential customer information using a new set of industry standards. Merchants who fail to follow the terms of these new guidelines may face liability for fines, liability for the fraudulent charges resulting from a data breach, and a revocation of credit card service, not to mention the bad press that goes along with a privacy breach.

Version 1.1 of the Payment Card Industry (PCI) Data Security Standard took effect Jan. 1, 2007, and was created by representatives from American Express, Discover, MasterCard, JCB and Visa International. Merchants who accept payment cards (both credit and debit) must establish a number of security procedures including:

- Maintaining a secure computer network, which includes installing firewall configurations;
- Protecting stored customer data;
- Encrypting customer data when it is transmitted;
- Restricting access to customer data on a need-to-know basis;
- Regularly testing security procedures; and
- Having a policy to address customer data security.

Some merchants also may be audited to ensure that they are meeting these new standards.

Ted Claypoole, a Womble Carlyle privacy and data security attorney, said that while technology such as firewalls can improve data security, proper procedures for employees are vital. Most security breaches take place because of human error, he said, and training employees in how to handle confidential customer information is a company's best defense.

Also, companies that fail to establish and enforce privacy procedures run the risk of lawsuits from customers should a security breach happen.

"If you don't have the right policies and procedures in place, you don't have an excuse if there is a security breach," Claypoole said.

Womble Carlyle currently is advising a number of retail and service clients on complying with the new PCI Data Security Standard. Our team of experienced privacy and data protection attorneys can help companies stay ahead of the new standards and avoid potential data security problems.

*~Over~*

**Ted Claypoole** – Ted is a senior member of the firm’s Intellectual Property Practice Group, with extensive experience in privacy and data security matters. He has worked with clients ranging from financial institutions to major manufacturers. Before coming to Womble Carlyle, he was Assistant General Counsel for Bank of America, where he was charged with protecting the company’s intellectual property. He has written about data security issues for a number of publications, including *Southeast Tech Wire* and the *Charlotte Business Journal*.

Phone: (704) 331-4910

Web: [www.wcsr.com/TheodoreClaypoole](http://www.wcsr.com/TheodoreClaypoole)

E-mail: [tclaypoole@wcsr.com](mailto:tclaypoole@wcsr.com)

**Mike Hubbard** – Mike is a nationally-recognized expert in the increasingly important field of privacy and data protection law. Mike’s vast practical experience in privacy and security matters includes negotiating privacy agreements and helping clients manage privacy concerns in a cost-effective manner. He also is a frequent speaker on privacy and data protection issues and has written extensively about these topics.

Phone: (919) 755-8126

Web: [www.wcsr.com/MichaelHubbard](http://www.wcsr.com/MichaelHubbard)

E-mail: [mhubbard@wcsr.com](mailto:mhubbard@wcsr.com)

***IRS CIRCULAR 230 NOTICE:*** *To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication (or in any attachment) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed in this communication (or in any attachment).*