MILLER CANFIELD

Protecting Your Consumers' Data: PCI Compliance as a First Step

March 12, 2012

Organizations that accept credit card payments have access to consumers' sensitive data and should be complying with the Payment Card Industry Data Security Standards (PCI DSS). A recent study by visa.com indicates that online sellers processing $20,000 to $1 million per year are only 60% compliant with PCI DSS. All sellers (both online and offline) processing less than $1 million per year are only moderately compliant with the standards.

The major credit card companies formed the Payment Card Industry Security Standards Council (PCI Council) in an effort to secure credit card and other sensitive data and to provide guidelines for sellers processing credit card payments. The PCI DSS requirements apply to anyone accepting, transmitting or storing cardholder data. Failing to maintain PCI DSS compliance could result in fines up to $100,000 per month, termination of processing rights and increased transaction fees.

The PCI DSS applies to businesses, both large and small. PCI DSS requires small-to-medium sized level 4 merchants to, at a minimum, successfully complete a PCI Self Assessment Questionnaire (SAQ) once a year. For businesses that also store payment card information electronically or use the internet to process payments, a quarterly scan by an Approved Scanning Vendor is also required. For the SAQ, merchants must also review, disclose and potentially remediate a host of requirements including: firewall configurations, physical access to cardholder information and test security systems and processing. With only moderate compliance being reported in level 4 organizations, those that are PCI DSS compliant may gain a competitive advantage by touting that fact to the consuming public.

Though the requirements of the SAQ will vary depending on the particular organization, the intent of the validation tool is clear: to protect consumers' payment card information, to avoid loss of reputation and to prevent potential financial liabilities and litigation. Small and large businesses alike that process payment cards should attain PCI DSS compliance. The costs to comply are low, but the risk for non-compliance and breach could be significant.

For more information on PCI DSS, visit the official PCI Council website. For strategies to comply with PCI DSS and other data protection laws that apply to your organization, contact your Miller Canfield attorney.