

LEGAL Q&A

Q My company intends to maintain credit card data from its customers. What are our data security obligations?

A Consider utilizing a third party vendor to process credit card information in order to limit liability. Alternatively, your company should comply with the Payment Card Industry (PCI) Data Security Standard. These extensive guidelines are created by the PCI Data Security Standards Counsel. The PCI Standards set six goals which are then focused into detailed security obligations: (1) Build and maintain a secure network and system; (2) Protect cardholder data; (3) Maintain a vulnerability management program; (4) Implement strong access control measures; (5) Regularly monitor and test systems; and (6) Maintain an information security policy. A sample of the compliance obligations are: installing and maintaining a firewall and anti-virus software; creating a personnel policy addressing maintenance and access to data; implementing software programs for encryption and tracking of data; regularly updating passwords and other security measures; and continually testing the system to locate weaknesses. As is evident in recent news stories, creating a secure system is not easily accomplished. Vendors should limit their exposure by complying with the PCI Standards.



Melissa V. Skrocki is a senior Associate at Giordano, Halleran & Ciesla, P.C. and member of the Intellectual Property & Technology and Corporate & Business Law Practice Areas. She can be reached at (732) 741 3900 or miskrocki@ghclaw.com.