

For many Ecommerce merchants processing orders and maintaining a website is an immense time-consuming step to growing a business. Grappling with PCI compliance and delving deeper into its origins, existence and proliferation are another daunting task to say the least.

Recently the NRF or *National Retail Federation* issued a merchant survey investigating PCI compliance and small online retailers. Out the polled group, 19% of non-compliant merchants said they had little to no understanding of this payment security process that is becoming increasingly imperative today in Ecommerce. Another 26% stated they lacked “the financial or technical resources to meet the standard, which covers a dozen broad areas from physical and network security to protecting” the CDE or cardholder data environment and maintaining commensurately structured security policies. Interestingly however, 86% of those polled claimed to feel somewhat familiar with PCI and its Ecommerce requirements.

A burgeoning problem for many merchants is that PCI standards evolve as do online threats and the emergence of security standards for making online transactions. New requirements are forced upon retailers in an effort to better protect cardholder spending money online. Analogously, PCI is implementing regulatory changes that will also affect payment processors and software providers. In summer 2010, new changes will occur that will dramatically affect both small online merchants and enterprise-size larger retailers alike.

-Pending PCI reqs.: any payment software handling cardholder data must comply with the PCI subset, Payment Application Data Security Standard...

-Pending PCI reqs.2: imposed by MasterCard, all merchants accepting credit cards online and in particular, those larger companies (level II merchants) must use 3rd party auditors to assess their PCI compliance

- **What does this mean?** For starters, smaller merchants will be taking on increased spending in order to remain compliant. Further, larger merchants will have to be assessed by outside parties and done so in a more stringent manner than previous iterations of PCI compliance mandated.
- **So how can merchants, small or large, reduce the heightened cost of Ecommerce and PCI compliance?** Internet Retailer and PCI KnowledgeBase advise not to store cardholder information if at all possible. Currently, under the PCI mandates, only “retailer systems, networks, servers, databases and software-that hold cardholder data fall under PCI.” Maintaining a strict and structured distance from the CDE will encourage PCI audit exclusion for Ecommerce merchants, small or large.

****Chart created from Internet Retailer, “Don’t Look Now.” Don Davis, Sept. 2009, p. 21****

PCI Level	Annual Transaction Volume	Internet Retailer no. of Merchants	Compliance Cost	Compliance %
1	6 million CC	362	\$450,000-4,400,000	93%
2	1-6 million CC	702	\$77,500-470,000	88%
3	20,000-1 million CC/Ecommerce	2634	\$19,250-72,000	57%
4	Under 20,000 Ecommerce; under 1 million total	6 million	Under \$5000	NA

