

12/14/2010

→ PCI Fines in Effect

Not PCI compliant? Better get going...companies are paying monthly non-PCI compliant fines.

There's been talk of non-PCI compliant fines since the standards were launched by the PCI Security Standards Council (PCI SSC) in 2006. We've seen companies suffering from a breach, like TJX Corporation in 2007, pay out bucket loads of money in fines, law suits and replacement credit cards. The cost of the TXJ breach has been estimated in excess of \$1 billion. But for years now, fines for non-compliance - as long as you don't suffer a breach - have seemed to be a relatively faraway threat.



That reality is quickly changing. We are seeing a growing number of non compliant PCI fines appearing on merchants' monthly bills from their acquirers. The fees vary depending on the volume of transactions. The average monthly non-PCI compliance fee we've seen falls between \$20 - \$25. We've seen a whopping \$1,000 non-compliant monthly surcharge. Ouch.

Payment brands have the ability to fine acquiring banks up to \$100,000 per month for non-compliance violations. These fees are then passed down by banks to non-compliant merchants. The potential costs associated with non-PCI compliance don't just end with fines, credit card replacement and audit fees: costs can also come in the form of loss of business and revenue, brand damage, increased transaction rates or banks terminating their relationship with a merchant. Such penalties can be catastrophic to a small business.

Complying with the requirements of the PCI DSS can be a daunting task both in terms of time and money to invest, especially for smaller companies. However, the costs associated with potential fines, business loss, and beginning to exponentially outweigh that of implementing PCI DSS.

If you need help taking the next step in achieving compliance, [contact us](#) and we can help get you started.