Why PCI DSS Compliance Matters

100 million shopper records; that's the latest total of customer records stolen from retailing giant Target. The episode, which included illegal access to 40 million debit and credit card records, was followed a few weeks later by the disclosure of another data theft from Neiman Marcus. And these are merely the latest in a series of incidents in which the records of merchants large and small have been compromised.

Thieves can employ an amazing variety of techniques to steal data at POS and ATM terminals or to directly or remotely infiltrate main servers. It's not just the "big boys" like Target who are in the criminals' sights: Anyone can be attacked. Even worse, small firms may be considered a soft target because they don't have big security budgets.

How can we better safeguard customer data? In part, the PCI Security Standards Council is working hard to enhance security to fend off fraudsters while emphasizing the importance of viewing security requirements as more than hoops to jump through. They hope to help merchants see the value of compliance as a way to truly protect their businesses and customers.

The Council's Data Security Standard (DSS) is being updated this year, from version 2.0 to 3.0, to reinforce defenses against increasingly sophisticated cyber-attacks.

Merchants can expect five major changes in PCI DSS in the next year or so:

- You'll need to perform more rigorous testing to verify that card data is segregated from other information. Companies that don't have in-house IT departments might need outside help with this step.
- You'll have to keep detailed records of all system components, including not only POS devices, computers and the software that runs on them, but also wireless access points.
- You'll also need to document how you and your vendors are working together to maintain security, clarifying where compliance responsibilities lie.
- Although you probably already have anti-malware software in place, you will need to extend its protection to areas normally regarded as less vulnerable.
- You'll need to isolate and protect physical access to POS devices to keep them safe from tampering and substitution.

These changes might seem challenging, but the new PCI requirements will not take full effect until next year. Remember, PCI compliance is not a choice, it's mandatory and your processor should help you navigate it: Security is everyone's responsibility and we are here to help. Contact Veracity at **(866) 944-0055** or at pcisupport@veracitypayments.com with questions.