PCIQ Why Comply with PCI Security Standards?

With version 3.0 of the PCI Security Standards taking effect in January, there has been more and more chatter about PCI. This month, we will focus on ensuring that you, as a trusted advisor, can accurately and completely articulate why your customers (merchants) should care about PCI Security Standards compliance. After all, at first glance, especially for small merchants, it may seem like a lot of effort. But not only is compliance becoming increasingly important, it may not be the headache you expected.

Compliance with data security standards can bring major benefits to businesses of all sizes, while failure to comply can have serious and long-term negative consequences. If asked by a merchant why it's important to comply with PCI Security Standards, here are some great responses:

1 **Compliance with the PCI DSS means that your systems are secure, and customers can trust you with their sensitive payment card information:**

- Trust means your customers have confidence in doing business with you.
- Confident customers are more likely to be repeat customers, and to recommend you to others.

2 **Compliance improves your reputation with acquirers and payment brands—the partners you need in order to do business.**

3 **Compliance is an ongoing process, not a one-time event. It helps prevent security breaches and theft of payment card data, not just today, but in the future:**

- As data compromise becomes ever more sophisticated, it becomes ever more difficult for an individual merchant to stay ahead of the threats.
- The PCI Security Standards Council is constantly working to monitor threats and improve the industry's means of dealing with them, through enhancements to PCI Security Standards and by the training of security professionals.
- When you stay compliant, you are part of the solution – a united, global response to fighting payment card data compromise.

4 **Compliance has indirect benefits as well:**

- Through your efforts to comply with PCI Security Standards, you'll likely be better prepared to comply with other regulations as they come along, such as HIPAA, SOX, etc.
- You'll have a basis for a corporate security strategy.
- You will likely identify ways to improve the efficiency of your IT infrastructure.

5 **Non-compliance could be disastrous:**

- Compromised data negatively affects consumers, merchants, and financial institutions.
- Just one incident can severely damage your reputation and your ability to conduct business effectively, far into the future.
- Account data breaches can lead to catastrophic loss of sales, relationships and standing in your community, and depressed share price if yours is a public company.
- Possible negative consequences also include: Lawsuits, Insurance claims, Cancelled accounts, Payment card issuer fines, Government fines and more. C

Test Your PCIQ:

1) **What is one reason that merchants should comply with PCI Data Security Standards?**

2) **What is one indirect reason that merchants should comply with PCI Data Security Standards?**

3) **Name one possible consequence for noncompliance.**

Answers on Pg. 33