Top 5 Myths About PCI Compliance

RELIABLE CARD SERVICE

As a payment processor for more than 27,000 merchants, we've heard an earful of PCI misconceptions. Here are the 5 most common:

1. **Myth:** We only take a small number of credit cards so we don't need to be PCI compliant.

Fact: Wouldn't this be nice? While it doesn't seem fair on the surface that a business would have to undertake PCI compliance for a relatively small number of transactions, it is required by the major card brands. The good news is that there are fewer PCI requirements for smaller businesses compared to larger ones. The merchant level that your acquiring financial institution or payment card brand assigns you will determine your PCI requirements. Level 1 merchants have the most requirements and level 4 merchants have the least. Regardless, there are consequences if the data you store or process is compromised no matter your transaction volume and merchant level.

2. **Myth:** I can just answer 'yes' to all the criteria on the Self-Assessment Questionnaire (SAQ).

Fact: Just like choosing "C" as the answer to every question on a multiple-choice exam won't get you a good grade, blindly answering "yes" to all SAQ questions won't get you PCI compliance. Most of the time, the self-assessment questionnaire serves as a guide for you to see what areas need attention in order for you to become compliant and protect your business. If a compromise took place and it was obvious that you were not adhering to PCI standards, the matter would be taken very seriously. In addition to being fined by the card brands, your business' reputation and sales could take a major hit.

3. **Myth:** You can never store cardholder data.

Fact: It is actually OK to store cardholder data as long as you encrypt it. The PCI Council advises that you only store it if it's absolutely necessary though. Cardholder data includes the primary account number (PAN), cardholder name, and expiration date. Conversely, data that should NEVER be stored is the sensitive data on the magnetic stripe or chip, or the card security codes printed on the front or back of cards. Learn more: https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf

4. **Myth:** I use a PCI compliant point-of-sale system, so therefore I am PCI Compliant.

Fact: Compliance cannot be achieved merely by purchasing a single solution or service. Using PCI compliant devices and applications is a requirement for PCI DSS Compliance, but it is only one component. Think about the other ways hackers or thieves could gain access to cardholder and sensitive authentication data. In addition to your device and applications, they could attempt to access the data through weak passwords, unaware employees, your corporate network, etc. That's why PCI DSS requirements encompass the entire transaction environment.

5. **Myth:** PCI is the law.

Fact: PCI is actually only enforceable by law in three states: Minnesota, Nevada, and Washington. However, PCI compliance is mandated by the card brands, and applies to all businesses that want to accept credit and debit cards. When a merchant accepts one card payment, it must abide by PCI and any additional provisions outlined by that card brand. If you don't follow the standards, you're increasing your risk of suffering a data breach and the card brands will likely fine you.