Education for You and Your Business

The Business Education Committee is proud to provide the Business Education article each month.

PCI Compliance – What It Is and Why You Should Care

By Tom Mansfield of ReliantPay, Inc.

On July 1, 2010 Visa and MasterCard began enforcing new rules for PCI DSS Compliance. If you accept credit cards you should be familiar with PCI Compliance. PCI Data Security Standards is a set of rules that help those accepting credit cards understand and take actions for any vulnerability that may exist in the methods a business uses to process and store credit card data. These are basic, common sense regulations developed by the brands such as Visa and MasterCard to help businesses ensure they are handling their customer information securely.

The creativity of the bad guys means businesses must constantly be on top of security. It's hard work for the crooks to rummage through trash cans in search of discarded credit card statements. The easiest method is to just tap into a company's system and grab card information that is electronically stored. The basic goal of PCI compliance is to ensure that these hackers are unable to get into your system and steal the data.

You may ask, "Why should I care about other people's credit card numbers"? You most certainly should care and consider the potential cost if one of these crooks obtains credit card information from your system or location. These potential costs include: paying for charges the crooks are able to make elsewhere, credit monitoring for the cardholders for up to a year, fines from Visa and MasterCard, the costs to upgrade the system that was breached, loss of business while systems are upgraded and investigated, costs to investigate the source of the breach, lawsuits from cardholders and perhaps attorney general, and the impact on your reputation after the breach. YOU are potentially liable for all of these items. As you can imagine, this liability can easily rise to hundreds of thousands of dollars.

So how do these new rules affect your business? Any business that accepts credit cards must take steps to be PCI Compliant. Certain terminals and software are now also considered "non compliant". There are also tighter encryption rules for debit pin pads.

What does it take to become PCI Compliant? Foremost, you need to ensure that your systems for processing cards are secure. This is done by answering a basic questionnaire that helps you affirm that you are taking reasonable steps to protect cardholder data. The questions and steps depend on the method you use to process. A dial out standalone terminal is considered the most secure and anything that transmits data over the internet is considered less secure (bad guys like less secure). Most of the PCI standards really are common sense steps such as making sure you have a firewall and antivirus software installed so the crooks can't deposit malware that will gather the credit card data from your system. PCI compliance also requires you to have test scans on your system every quarter to ensure the crooks can't hack into your system. Thus there is a double benefit as you can be more certain your entire systems are secure

.

Any business has certain responsibilities to your customers. One of those responsibilities is to assure customers that they can trust a business with personal information. This includes ensuring the business is securely sending and storing customer credit card data. PCI Compliance is one way for customers to

remain confident that privacy is taken seriously. Feel free to contact our office at 314-651-1260 for an update on the requirements to keep your customer's data secure.

Tom Mansfield is a chamber member and president of ReliantPay, Inc., a local credit card processing company that is a registered ISO of Visa and Master Card. He can be contacted at (314) 651-1260.