The Dangers of Failing to Be PCI Compliant

Payment Card Industry Data Security Standard (PCI DSS) has been a topic of conversation among creditors since entering the business-to-business landscape more than a decade ago. NACM's recent webinar titled "PCI Compliance and What Your Company Needs to Do to Get There" delved into the nuances of PCI compliance, breaking down any misconceptions and providing context for how to get companies to be the most efficient and PCI compliant as possible.

If a company accepts credit cards, it must be PCI compliant. The business can have a staff as large as 50,000 or as small as one person—should credit cards be an accepted form of payment, the company must practice PCI compliance.

PCI compliance has roots in security, namely for protection against data breaches. The compliance is a "set of standards developed to ensure that the credit card industry is securing customer data uniformly throughout the industry," said Ronald Sereika, CCE, CEW, the host of the webinar. The idea to create a set of rules for security came into fruition in 2006, when data theft became a recurring phenomenon. The advent of the internet changed the landscape for payments, breaking down walls of security for businesses and consumers.

The PCI Security Standards Council, developed soon after payment concerns arose in 2006, was led by Visa, MasterCard, Discover and American Express. This then prompted the creation of the PCI DSS, which helps regulate and secure credit card transactions through a set of rules. While the rules are not beholden to laws, they still pose substantial weight within companies.

"The PCI security standards designed by the credit card companies are industry rules, not laws," Sereika said. "However, if these standards are not followed, they could result in stiff fines and penalties for any business."

The PCI-DSS requirements are broken down into three categories: data security policies, data handling policies and the destruction of credit card data from processing systems. Payment data, according to Sereika, includes the full primary account number (PAN), the card holder's name and the CVV code and expiration date.

For example, should a creditor jot down any credit card information manually on a notepad or Post-It note, the creditor is responsible for destroying the paper. Leaving the number out poses a risk for the customer, which may lead to a breach, should the wrong person find the note.

The level of PCI requirements held by a company depends on its annual transaction volume—not the amount of revenue. One company can earn $100 billion a year and process one million transactions while another can earn $80 billion a year processing three million transactions, and the latter company will be held to a higher level of PCI compliance than the former.

But the level of compliance can change, should a company fail a breach.

"If your company fails a breach, the security standards board has the right to change your level standard to a stricter level, regardless of the number of transactions processed per year," Sereika said.

While the PCI can be intimidating, Sereika discussed actions creditors can take in order to be more PCI compliant.

Merely educating staff on the importance of PCI compliance can help weaken the risk of a breach; this includes working with the IT department. Working with the IT team to figure out where and how credit card information can be stored can help with PCI compliance. Maintaining open avenues of communication, like with any serious matter in the office, can be the most important step.

Working with customers can strengthen PCI compliance as well. Requesting customers to never email credit card information or leave information in a voicemail reduces the risk of a breach. While each company is responsible for a customer's information, the customer must also act responsibly.

"PCI compliance applies to all businesses, regardless of size, that accept credit cards," Sereika said. "… PCI compliance for small businesses lessens the liability for your business when a data breach occurs."

—Christie Citranglo, NACM editorial associate