New Year's Cyber Security Resolutions: PCI Compliance

January 8, 2018

Industry experts estimate that a growing number of businesses, from start-ups to middle market companies have an increased risk of having a cybersecurity issue. Making sure that you understand compliance standards and take appropriate action in the event of an issue is critical.

By all appearances, retailers are celebrating the close of this Holiday Season. MasterCard, Inc. has estimated that consumers spent $800 billion between November 1 and December 24, amounting to a historic high water mark of spending - a 4.9% increase over last year. With the vast majority of these transactions being conducted via credit-cards, it is critical for online and traditional retailers to be aware of their cybersecurity risk profile, specifically the devastating financial implications that can result from Payment Card Industry (PCI) compliance fees resulting from a data breach. No retailer is immune to cybersecurity risk, and those that aren't paying attention to PCI Compliance Fees risk a future visit from the "Grinch Who Took Last Year's Profits".

What is PCI Compliance?

PCI stands for the Payment Card Industry. PCI is a trade group of credit card companies that created cybersecurity standards and best-practices in an effort to self-regulate and avoid government involvement.

Who is subject to PCI Compliance regulations?

In short, any retailer that accepts credit cards is subject to PCI compliance regulations, as part of their credit card company merchant agreement. Any retailer who accepts credit cards signs a merchant agreement in order process credit card transactions. Buried within this agreement is language that your business promises to abide by the PCI standards and practices established by the credit card company.

What happens if I am not in compliance with the PCI standards?

A retailer that fails to abide by PCI standards, could be fined by the credit card company if they were to experience a cybersecurity or data breach. These fines can be up to $100,000 and are based on the number of impacted records and other factors. Retailers whose computer or Point of Sale system is infected with a virus that steals a significant amount of credit card data (generally over 10,000 cards) will be fined by the credit card company on a per-card basis if the retailer is not PCI compliant and otherwise fails to follow PCI procedure.

Can you give me an example of what happens to a merchant that is not PCI Compliant?

Example: A restaurant's point of sale system is infected with a virus that steals 40,000 AMEX credit card numbers over a period of time, and AMEX determines that that restaurant is not PCI compliant. Amex assesses the restaurant a fine up to $5 per card, or $200,000. The fine schedule and its explanation are located in AMEX's Data Security Operating Policy, which is referenced in the Merchant Agreement. With appropriate help from advisors, the amount of the fine can sometimes be negotiated, but the retailer will likely end up paying a significant amount.

What if the data breach isn't my fault?

With the resurgence of our economy and the boom in online sales, there has been a staggering increase in data-security breaches. Reports of cyber-theft have become commonplace – to the point that we have become immune to the often shocking amount of credit-card thefts that have occurred. In order to combat the significant increase in credit card theft, credit card companies have enhanced their fraud and abuse programs. Who pays for this? You do. If you are a business that accepts credit cards and you fail to be PCI compliant, the credit card companies will fine you if a data-incident occurs in your business because of your failure to comply. The cyber breach may not be your fault – and it most often is not. Your Merchant Agreement, however, obligates you to pay.

What remedies do I have against the credit card companies?

Right now you may be thinking that suing the credit card companies could be a possible remedy. But, not so fast. Your Merchant Agreement also requires you to submit to binding arbitration for any disputes. And if you lose, you have agreed to pay the attorney's fees for the credit card companies. These terms apply to every business, from Amazon to the mom-and-pop corner store.

What can I do right now to protect my business?

A little prevention just may save last year's profits. With the upcoming New Year, consider embracing the following New Year's resolutions to help understand PCI compliance and take steps to make sure that your business is not at risk for PCI fines.

2018 PCI / Cybersecurity New Year's Resolutions

1. I will read the Merchant Agreement for each credit card I accept;
2. I will read the Data Security Policies for each of the credit card companies with whom I do business;
3. I will ask questions if I do not understand what is contained in the Merchant Agreements and/or the Data Security Policies;

4. I will take steps to find out if I am PCI complaint;
5. If I am not currently PCI compliant, I will find out what I need to do to become PCI compliant; and
6. I will save my profits by becoming PCI compliant.