

EMS: Why PCI Compliance Is A Necessary Ingredient For Commercial Success

February 28, 2022

Cleveland, Ohio - February 28, 2022 - PRESSADVANTAGE -

Cleveland, OH based Electronic Merchant Systems (EMS) is taking steps to educate the business community about the importance of PCI compliance. As an expert in the field of secure payment protocols, EMS has a wealth of insight to share on the subject.

In a nutshell, PCI compliance has to do with data security, specifically the security of customer data regarding credit cards. Since credit cards represent a fundamental aspect of how the average business conducts transactions with customers in the US, this is a component of their overall security profile that they cannot afford to ignore. In regulatory terms, if the business in question accepts credit card payments, they must both achieve and maintain compliance with the PCI Security Standards Council (PCI SSC).

EMS explains that the PCI Security Standards Council was founded more than a decade ago with the objective of helping merchants and financial institutions to secure their payment systems against loss or malicious breach (such as in cases of data theft). The organization also makes it a point to educate vendors on industry standards for creating secure payment solutions. To become compliant with the Payment Card Industry Data Security Standard (PCI DSS), these vendors must maintain a secure environment if they process, store or transmit credit card information.

Failure to uphold these standards can lead to the business receiving heavy fines on top of losing the trust of their customers and partners, among a host of other consequences. Electronics Merchant Systems points out that businesses which demonstrate an inability to secure their customers' credit card data will likely have to contend with losses due to fraud; reduced sales and legal costs, settlements and judgments, among other drawbacks. Depending on how extensive the violation is (and how capable the company is of bringing themselves back into compliance), they may even lose their merchant account altogether. In a world where customers expect convenient payment options from their preferred businesses, this can be a crippling blow. In time, they may even go out of business.

Notably, PCI DSS compliance is not a legal requirement (though certain state laws do address some aspects of the field). However, most businesses will find it necessary to remain in compliance if they wish to work with a major payment card network. EMS advises that compliance with PCI standards be considered an investment in the business' future. In addition to avoiding the aforementioned consequences, compliance also offers several benefits, not the least of which are better security and the ability for the business to partner with card issuers to launch their payment card. EMS adds that customers are also more likely to favor businesses that have no history of data security breaches.

EMS states that there are 12 PCI requirements for PCI DSS compliance. Each requirement may have hundreds of sub-requirements, and a business has to complete all 12 overall requirements in order to become compliant. The company notes that some of these requirements are relatively easy to handle, such as never using vendor-supplied defaults for system passwords or other security parameters. However, others may represent a significant challenge to certain organizations, especially if they do not have dedicated data security departments or partners that can take on such responsibilities on their behalf. Installing and maintaining a firewall configuration to protect cardholder data, for instance, can be difficult without the relevant tools and expertise, especially since maintenance is an ongoing task.

There are four distinct levels of PCI DSS compliance, and each is based on the number of credit card transactions the business in question processes each year. Level 4 is the least stringent of these (and also the least expensive) as it applies to businesses that handle 20,000 e-commerce card transactions per year (or up to 1 million regular card transactions per year). At the other end of the spectrum is Level 1, intended for businesses that process over 6 million card transactions per year. EMS points out that any business that suffers a data breach is also required to 'upgrade' to Level 1 as a result. This may have a relatively larger impact on small and medium-sized businesses since this level can cost \$50,000 a year or more. Therefore, it is in their own best interests to do everything in their power to remain PCI compliant and minimize the risk of data breaches.

Electronic Merchant Systems recognizes that this is a complex topic that can add to the stress of running a business. Fortunately, a viable alternative exists that any business can opt for: to partner with a reputable payment processor like EMS. By doing so, they will be better equipped to maintain PCI compliance while streamlining operations and improving the customer experience. Learn more about payment security at EMS.

Further details on PCI compliance can be found on EMS' blog space. Those interested in utilizing the company's services may also contact the EMS team directly via phone or email.

###

For more information about Electronic Merchant Systems, contact the company here:Electronic Merchant Systems(800) 726-2117info@emscorporate.com250 W Huron Rd #400Cleveland, OH 44113

Electronic Merchant Systems

Established in 1988, Electronic Merchant Systems has grown to become a leading provider of payment processing & merchant services. Electronic Merchant Systems' mission is to be the industry leader in merchant services and payment processing solutions.

Website: <https://www.emscorporate.com/>

Email: info@emscorporate.com

Phone: (800) 726-2117



Powered by PressAdvantage.com