REVENTION™

IS YOUR ONLINE ORDERING PCI COMPLIANT?

Common Myths of Online Ordering PCI Compliancy

WWW.REVENTION.COM

Introduction

There are many misconceptions out there regarding PCI compliancy and online ordering websites. There is no magic bullet fix to secure an online ordering website from vulnerability. To protect your customers from credit card fraud and identity theft it is necessary you select an online ordering solution that actively complies with the PCI Data Security Standard (PCI DSS). Selecting an online ordering service that is not truly PCI compliant is like not locking the front door of your business before you go home at night. Read the following myths to understand how to validate your online ordering solution is truly PCI compliant.

Myth 1: My online ordering company says they are PCI compliant, so they must be.

When asked, most online ordering companies will state they are PCI compliant, but whether they have truly completed and fulfilled all of the requirements requires scrutiny. The most sure fire way to validate your online ordering service provider has fulfilled the PCI DSS requirements is to find them listed on the two major card brand websites as certified PCI compliant service providers.

A breach of a service providers' network is a breach in your network. Any card data processed by your customers through the website is potentially at risk. Your business reputation and customer's data security is at stake.

Check the official card brand PCI compliant service providers list.

http://www.visa.com/splisting/searchGrsp.do

http://www.mastercard.com/us/company/en/whatwedo/compliant_providers.html

Myth 2: I don't run enough online credit card transactions to require PCI compliancy.

Wrong. Whether you run 6 or 6 million credit card transactions, PCI compliancy is required for any public facing website. Following the PCI DSS requirements is critical to the security of your online ordering customer's credit card data. Intrusion risks are higher for public websites.

Myth 3: The data center that hosts our online ordering website is PCI compliant.

A PCI compliant data center is an important requirement, but it does not fully address all 12 PCI DSS requirements. When a service provider focuses on one aspect of compliance it is typically meant to give a perception of complete compliancy when in reality the PCI standards go much deeper. What part of a data center can protect the website from a computer programmer hacking the site and extracting data? What ensures your online ordering provider has not mistakenly hired a crook that has a added a back door to all of your online ordering data? Complete PCI compliancy of an online order service provider will include validation of all 12 PCI DSS requirements.

Myth 4: I am a small company, PCI compliancy does not pertain to me.

Wrong. Any entity that processes, stores, or transmits credit card data is subject to PCI DSS requirements. Many times the small companies are more vulnerable because of this misconception. Is your online ordering provider a small company too? Then be even more concerned, they too are potentially a more vulnerable target. A computer crook is not concerned with who they obtain the data from, it's about how easy it is to get to the data.

Myth 5: My online ordering provider showed me their Attestation of Compliance, so that means they are compliant.

An Attestation of Compliance is a downloadable form that can be found on the PCI Security Standards Council (PCI SSC) website. The truth is any online ordering company can complete a PCI DSS Self-Assessment Questionnaire (SAQ) and a Attestation of Compliance (AOC) but the most reliable method of becoming PCI compliant is to have that information validated by an independent Qualified Security Assessor (QSA). A QSA must adhere to the PCI SSC requirements and are themselves certified to be a Qualified Security Assessor by the council. Sounds complicated, right? But it is pretty simple, your online ordering company contracts a QSA to validate they are following all of the 12 PCI DSS requirements. By having an independent validation of the online ordering company's PCI compliance you will know that the requirements are in place.

Myth 6: My online ordering company says they are compliant and have been certified by a Qualified Security Assessor.

One simple question remains, **when will they be listed on the major card brand sites?** If all of the requirements have been fulfilled and the paperwork is complete, it is a no brainer. Register with Visa and Master Card and put an end to any question.

Myth 7: Using a third party payment gateway eliminates an online ordering provider's PCI DSS requirements.

Many payment gateway providers are available in the market today, and if part of your service provider's solution must also be certified PCI compliant. Using a payment gateway does not change the requirements related to the online ordering provider compliancy. The credit card number is still being entered in the public facing website and transmitted to the payment gateway. This still places responsibility on the online ordering provider to meet the PCI DSS requirements.

Myth 8: My online ordering solution does not store credit cards, so PCI compliancy is not required.

Storing credit cards does make PCI compliancy a more rigorous process. All entities that store, process or transmit cardholder data are required to comply with the PCI DSS requirements and validate their compliance in accordance with the payment brands' compliance programs.

Myth 9: My hosted online ordering website has an SSL certificate, so the website is secure.

SSL certificates do not secure the Webserver from malicious attacks or intrusions. A high assurance SSL certificate provides the first tier of customer security and assures a secure connection between your customer's web browser and the web server for the online ordering service. The SSL certificate also validates the website operators is a legitimate, legally accountable organization.

Myth 10: I receive my web orders via fax or email, so PCI compliancy is not required.

The only way this statement is true is if you do not accept credit cards at all online. If your online ordering service provider accepts credit cards on your behalf and processes them it is still required for your financial and reputational security to use a PCI compliant online ordering solution.

Myth 11: The worst thing that can happen is they shut my online ordering site down.

That is just the beginning. The card brands can fine you based on the number of cards compromised that are traced back to your business, they can prevent your business from taking credit cards, they can require you to pay for a costly forensic audit, your own brand damage and loss of revenue. Loosing your business should not be an acceptable risk. It is easy enough to select a certified PCI DSS complaint online ordering solution.

Conclusion

The final misconception by merchants is the premise it will never happen to them. It will happen , it is just a matter of time if you are not doing everything in your power to follow the rules and standards of PCI compliancy. The simple truth is if you the merchant are following the PCI DSS requirements and fraud does occur, you may not be considered liable. Being PCI compliant does not necessarily guarantee you will never experience a breach. It does guarantee you have done everything in your power to protect your customers' cardholder data.