



# Merchants Often Confused by Complex Credit Card Security Requirements

*Credit Card Security Standards create requirements for businesses that accept credit cards; complex requirements include over 400 confusing control objectives.*



EVERETT, WASHINGTON, USA, March 21, 2015 /EINPresswire.com/ -- Organizations that store, process, or transmit credit card data must comply with industry regulations established by the Payment Card Industry Security Standards Council (PCI SSC). The PCI SSC established the Data Security Standard (DSS) for credit cards and is endorsed and accepted by card brands such as Visa, MasterCard, American Express, and Discover. The standards are designed to minimize the potential for credit card fraud and theft; however, for many merchants, the confusing requirements make complying with PCI DSS extremely difficult. This difficulty may, in fact, increase the possibility of non-compliance leading to increased credit card data exposure.

InfoSecure, the nation's leading resource for credit card security professional services ([www.InfoSecureIT.com](http://www.InfoSecureIT.com)), has helped thousands of merchants and other organizations comply with PCI DSS using innovative and cost-effective solutions designed to save businesses time and money. "There are over 400 control objectives that businesses must comply with in order to achieve PCI DSS compliance," said Patrick Bass, InfoSecure CEO and Founder.

Bass knows a thing or two about credit card security, he's been helping organizations comply with PCI DSS since 2004 and is a PCI SSC certified Qualified Security Assessor (QSA) and states, "We started InfoSecure because we saw a huge need to help merchants that want to make sure their customer's credit card data is secure, but don't have the experience or resources needed to comply with PCI DSS."

The company is the creator of the original PCI DSS [Policy](http://policytoolkit.infosecurepci.com/) ToolKit, a low-cost policy template package that includes all of the policies, procedures, forms, tools, [training](#), and other material needed by organizations for compliance with PCI DSS. "We set the price point at \$375 to ensure that this material was available to any business that needed it. Sure, we could charge two or three times this amount, and many knock-offs offer lower quality documents at a much higher price; however, we believe in providing high quality work at fair prices," remarked Bass. InfoSecure is so sure of their product that the company offers an unprecedented money back guarantee and 60 days of support from a PCI QSA. The PCI Policy ToolKit is available for immediate download at <http://policytoolkit.infosecurepci.com/>.

InfoSecure is a full-fledged consultancy and offers many other services and solutions. Recently, the company launched its online Learning Management Systems (LMS) which provides multimedia-based information security training for employees. "What makes our system unique is that we target the training based on job roles. For example, we have a training program for employees that operate point-of-sale terminals. It provides all of the training required to comply with PCI DSS learning requirements, takes about 30 minutes to complete, and is only \$19 per student," explained Bass. "We have other programs available with several more in development. Plus, the system provides full

compliance tracking and we offer group discounts.” To find out more about InfoSecure’s Learning Management System, visit <http://training.infosecurepci.com>.

One other area where merchants have a very difficult time achieving compliance with is the PCI DSS requirement for [penetration](#) testing. The standard requires both an internal and external penetration test. Pentesting, as it is often called, is substantially different from vulnerability scanning, another PCI DSS requirement. During pentesting, InfoSecure’s team of Certified Ethical Hackers seek to identify and exploit vulnerabilities in a controlled environment using the same techniques that malicious hackers might use during a real attack. “Our exclusive techniques meet all of the requirements of PCI DSS, plus, we identify any areas where unencrypted credit card or magnetic stripe data are stored insecurely,” stated Bass, “we find the issues and help businesses fix them before the bad guys can steal data.” Prior to InfoSecure’s innovative approach, organization’s often paid thousands of dollars for this complex assessment; however, InfoSecure’s approach offers the same quality and results for a fraction of that price. For more information, visit <http://www.infosecureit.com> and click on Services > Penetration Testing.

InfoSecure is leading the charge in helping businesses comply with PCI DSS, Experian’s data security requirements, and International Standards such as ISO 27001/27002. The business is currently based in Everett, Washington with expansion plans for San Antonio, Texas during April 2015. “We are growing due to our aggressive pricing strategy and high quality. We have amazing business partners and the best clients in the world,” Bass said. For more information visit <http://www.infosecureit.com> or call the InfoSecure toll free at (877) 674-6965.

Patrick Bass  
InfoSecurePCI  
877-674-6965  
[email us here](#)

---

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.

© 1995-2015 IPD Group, Inc. All Right Reserved.