PCI DSS 3.1

How Merchants Can Improve Their Productivity and Security Through the New Compliance Standards

NETBANX®

Executive Summary

The Payment Card Industry Security Standards Council (PCI SSC) has further tightened security requirements with respect to online payment processing with the launch of Payment Card Industry Data Security Standards (PCI-DSS) 3.1 standard.

With card payment fraud on the rise, the newly introduced requirements have been strengthened compared to previous PCI-DSS versions, with a focus on e-commerce merchants using web redirects.

However, the stricter requirements are also an opportunity for the merchants to provide a security enhanced payment option to their customers, optimize their IT resources, and in turn enhance their productivity.

This report takes a look at why PCI-DSS 3.1 is a good investment for merchants and what steps they need to take to be compliant.

Online Fraud is On the Rise

Credit card fraud has become one of the largest issues in ecommerce today. According to a 2015 report from Barclays, 47% of the world's credit card fraud happens in the United States, and U.S. credit-card-fraud losses totaled roughly $18 billion in 2013, according to Javelin Strategy & Research.

Small- to medium-sized businesses (SMBs) are particularly vulnerable due to a lack and even a decrease of investment in online security measures in recent years. According to PwC's Global State of Information Security Survey 2015, compromises of mid-size firms rose 64% from 2013 to 2014.

While the looming North American deadline for the conversion of magnetic-stripe payment cards to the security-enhanced Europay-Mastercard-Visa (EMV) chip card will undoubtedly reduce the account data compromise risk at the point-of-sale (POS), this in turn would potentially impact card-not-present (CNP) transactions.

Research and consulting firm Aite Group estimates U.S. online card fraud will more than double to $6.6 billion from $3.3 billion between 2015 and 2018.

It is therefore even more relevant and important today for merchants to ensure that they remain vigilant and are compliant with the Payment Card Industry Data Security Standard (PCI-DSS).

What is PCI?

PCI-DSS was created more than a decade ago by the PCI Security Standards Council, an entity founded by Visa, MasterCard, American Express, Discover, and JCB, global payment brands to protect cardholder data and alleviate merchant-based vulnerabilities that may appear at all points in the payment card processing ecosystem.

Numerous companies – from banks to payment processing vendors – may be involved in the transaction process; however it is ultimately the merchant's responsibility to ensure compliance and protect the consumer's data.

PCI compliance formally requires merchants to establish and implement standard security policies, procedures and controls to avert the theft of cardholder data. While small-to-medium merchants are required to maintain their PCI-DSS compliance at all times, especially when making changes to key personnel or changing/introducing new processes or systems that touch payments, they must only attest to that fact annually – usually, by completing a Self-Assessment Questionnaire (SAQ).

Any entity that stores, processes or transmits cardholder data – from multinational retailers to the corner pizzeria -- must comply and adhere to PCI-DSS standards. The level of specificity and scrutiny depends on the size of the company's annual payment card processing volume and the scope of the work they undertake. A useful guide to further understanding the requirements of PCI-DSS and which validation route suits your business, can be found at https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

For ecommerce merchants that accept payment cards for transactions, PCI-DSS certification is an essential and vital aspect of business management – as important as marketing and distribution.

Without PCI-DSS certification and compliance, a company and its customers are highly susceptible to cyber-attacks. Non-compliance means the company may be subject to fines, penalties and termination of the right to accept payment cards which can lead to loss of business.

PCI DSS 3.1 – The Latest Standard

Several PCI-DSS versions have been released over the years to provide updates in order to keep-up with evolving ecommerce practices as well as cyberattacks. PCI-DSS 3.1 is the current and latest data security standard released by the PCI-SSC **to address a security vulnerability in SSL (Secure Socket Layer), a common method of sending sensitive cardholder data over the internet.** This latest version has much more specific and detailed requirements compared to previous PCI-DSS versions, and puts more of the onus of compliance – and the consequences of non-compliance -- on the merchant. With PCI 3.1, the level of care required by merchants to achieve compliance has become more rigorous **as the result of the new heightened security protocols.**

According to the PCI Security Standards Council research, just one in 10 merchants that had previously achieved full compliance with earlier versions of PCI-DSS remained so at the time of their next re-assessment. Further, many merchants who experienced a data breach had achieved compliance during their most recent PCI-DSS assessment, but had subsequently lapsed.

As the Council states on its website, "PCI-DSS 3.1 helps organizations focus on security, not compliance, by making payment security business-as-usual." While that is indeed true, companies should not underestimate the level of complexity and time required to implement PCI 3.1, especially for SMBs with limited in-house IT resources.

While the entire scope of PCI 3.1 involves dozens of clarifications and additional requirements, the key changes in PCI 3.1 are:

- SAQ Completion for most SMBs – Most SMBs fall into a PCI 3.1 compliance level that mandates they complete an SAQ to attest to their validation with all requirements.
- More time is required during the assessment - Whether completing a self-assessment or – in some cases – working with a Approved Scanning Vendor (ASV) or Qualified Security Assessor (QSA) to complete vulnerability scans or other necessary tasks, most companies are wise to begin the re-certification process well before their annual compliance anniversary date.
- More costs incurred through compliance requirements – While compliance expenditure levels vary considerably depending on the size and scope of a company's operations, many merchants may underestimate the additional IT and vendor costs required to achieve full compliance.

PCI 3.1 Can Help Merchants with Payment Security as well as Productivity

Smart merchants have understood that complying with the requirements of PCI 3.1 can be a business advantage. Several of the requirements support and even enhance a merchant's business productivity and growth by adhering to the security measures of PCI 3.1.

Some of these include:

De-scoping

The scope of a merchant's card payment process is often misunderstood. PCI 3.1 forces merchants to identify every step in an ecommerce transaction, beginning with the online payments page environment and extending through every department, vendor and bank that touches the customer's payment card information.

When determining the scope of its payment environment, a merchant may discover it is

taking on too much of the payment processing responsibility. Many SMBs that have customized their ecommerce payment page using their own servers are employing Direct Post Method (DPM) to process card payments. DPM – for which merchants maintain complete control of payment page design and data fields -- often includes the storage of cardholder data for repeat or recurring transactions. While the merchant retains more control using DPM, its internal IT resources and servers bear more responsibility for processing and securing customer card data. This can mean more risks, threats and vulnerabilities for hackers to exploit and steal sensitive data.

As a result, merchants may wish to consider de-scoping aspects of the card payment process – including DPM – and outsourcing them to an approved third party online and mobile payment processing company that operates a secure payment gateway.

Not only will de-scoping ensure a higher level of security and decrease the likelihood of hacks, but it greatly reduces the merchant's PCI 3.1 certification responsibilities.

Tokenization

Another operational change that can lower the risk of fraud is to employ tokenization as part of the payment processing scheme. Through tokenization, payment card numbers are replaced with a randomly generated series of numbers, letters, or alphanumeric that are issued only once and called "tokens," which are useless to hackers, as they cannot be used to make fraudulent purchases. As with de-scoping, tokenization also significantly reduces PCI 3.1 compliance and requirements and liability for the merchant.

Eye-Opening Security Opportunities

The heightened requirements associated with PCI 3.1 are prompting most ecommerce merchants to thoroughly audit and evaluate their existing operations procedures and security protocols. What they are finding is often revealing, with many discovering that they may not be nearly as secure as they thought.

Better Security, Guaranteed

The gauntlet of steps a company is required to navigate in order to assess, comply with and attest to the numerous PCI 3.1 requirements will undoubtedly leave them more secure than ever. Everyone in the ecosystem benefits from an in-depth multi-layered protective system that enables ecommerce to be conducted expeditiously, accurately and with the utmost protection.

Reputation Protection

PCI 3.1 compliance may not completely eliminate vulnerability to hackers, but the absence of obvious weaknesses in the payment processing ecosystem will frustrate the bad guys – who will quickly search elsewhere for victims. No breach means no bad press, and an intact corporate reputation.

Twelve PCI-DSS requirements to protect your business and customer data

Designed to mirror best practices in security and fraud management, the 12 PCI-DSS 3.1 requirements include a series of practical steps merchants should take to achieve compliance and ensure their payment processing practices are airtight, always.

Security Goals	12 PCI-DSS Requirements
Build and Maintain a Secure Network	1. *Install and maintain a firewall configuration to protect cardholder data.* 2. *Do not use vendor-supplied defaults for system passwords and other security parameters.*
Protect Cardholder Data	3. *Protect stored cardholder data 4.* 4. *Encrypt transmission of cardholder data across open, public networks.*
Maintain a Vulnerability Management Program	5. *Protect all systems against malware and regularly update antivirus software or programs.* 6. *Develop and maintain secure systems and applications.*
Implement Strong Access Control Measures	7. *Restrict access to cardholder data by business need to know.* 8. *Identify and authenticate access to system components.* 9. *Restrict physical access to cardholder data.*
Regularly Monitor and Test Networks	10. *Track and monitor all access to network resources and cardholder data.* 11. *Regularly test security systems and processes.*
Maintain an Information Security Policy	12. *Maintain a policy that addresses information security for all personnel.*

Source: PCI Security Standards Council, Requirements and Security Assessment Procedures, https://www.pcisecuritystandards.org documents/PCIDSS_QRGv3_1.pdf

Finding the Right Partner to Support PCI 3.1 Compliance

How can a merchant sort through the maze of vendors and partners offering consulting services regarding PCI 3.1 certification and compliance activities? The best way is to start with trusted partners.

Every merchant must engage a payment processing company which serves as a secure conduit between the banks, payment card providers and other links in the ecommerce chain. The best gateway companies are PCI-DSS Level 1 certified, the highest level of compliance in the industry.

PCI-DSS Level 1 certified partners have the resources and the expertise to offer consultative services for merchants throughout the PCI certification process. The NETBANX online payment gateway and payment processing services platform Optimal Payments has successfully – and securely - processed billions of payment card transactions for over a decade. The company also works with a number of partners that specialize in PCI Qualified Security Assessments (QSAs) and experts that can walk merchants through every stage of the PCI-DSS compliance process.

One of the best in the US is SecurityMetrics, a leading provider and innovator in data security and compliance for organizations worldwide, which can conduct vulnerability scans, penetration tests, audits, remediation and other hands-on services that enable ecommerce merchants to gain – or regain – PCI-DSS compliance. Trustwave is one of the leading providers in the UK.

In summary, SMBs who view PCI-DSS re-certification as another in a long list of tasks are missing out on an opportunity to incorporate it as a key clue in solving an increasingly complex IT security puzzle.

PCI 3.1 must be seen for what it truly is: an opportunity to holistically review, assess, update and operationalize a robust, company-wide security and fraud management system that prompts hackers to look elsewhere for the next victims.

For more information, please contact us at **sales@netbanx.com** or visit our website at **www.netbanx.com**

About Optimal Payments

Optimal Payments is a global provider of online payment solutions, trusted by businesses and consumers in over 200 countries and territories to move and manage billions of dollars each year. Merchants use the NETBANX® platform and services to simplify how they accept credit and debit card, direct-from-bank, and alternative and local payments; and the NETELLER® service to increase revenues and capture new customers. Consumers use the multilingual and multicurrency NETELLER and Net+® Card stored-value offering to make secure and convenient payments. Optimal Payments Plc is quoted on the London Stock Exchange's AIM, with a ticker symbol of OPAY. Subsidiary company Optimal Payments Ltd is authorised and regulated as an e-money issuer by the UK's Financial Conduct Authority (FRN: 900015).