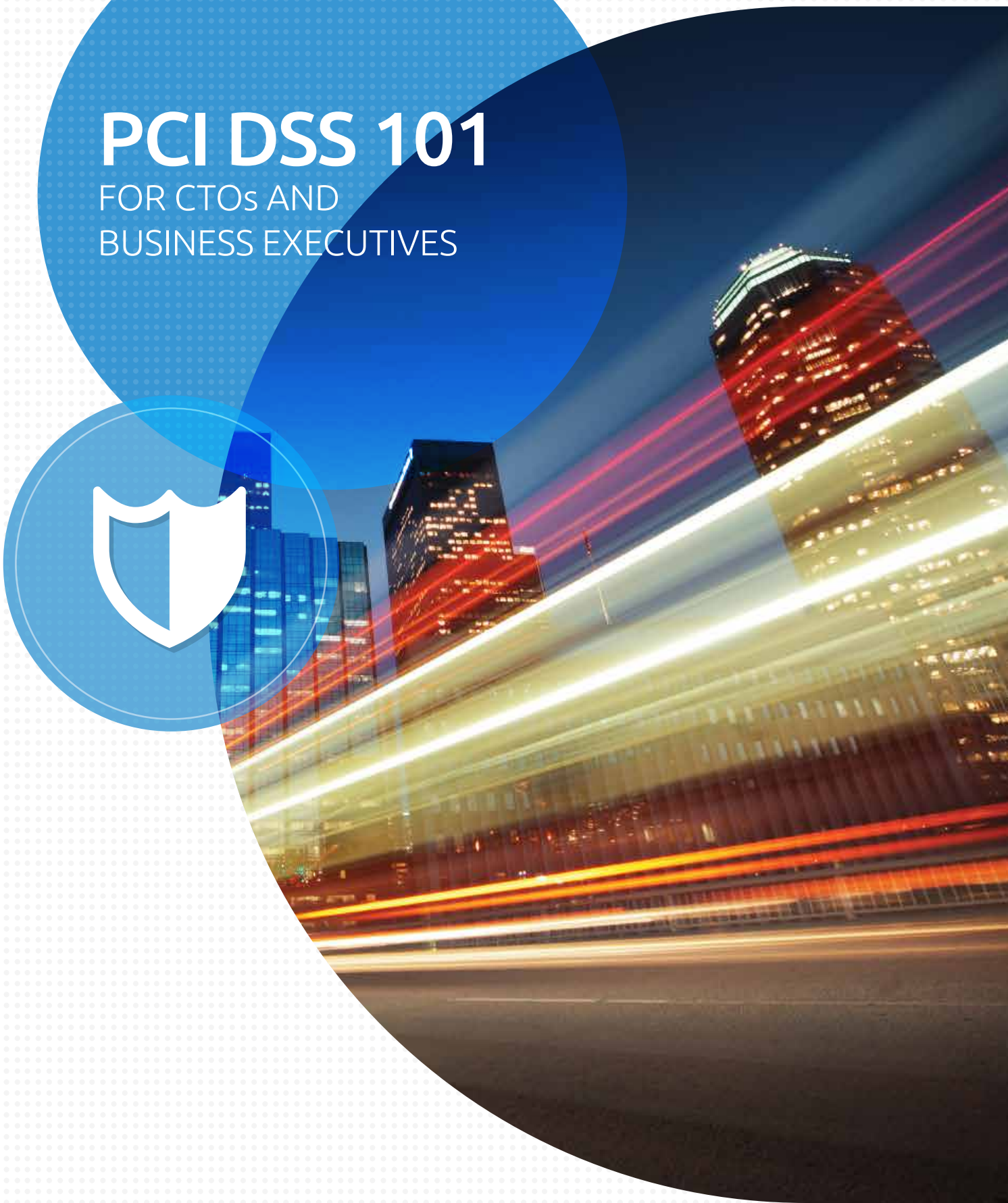
ecentric
PAYMENT SYSTEMS

PCI DSS 101

FOR CTOs AND BUSINESS EXECUTIVES



CUTTING THROUGH
THE COMPLEXITY AND CONFUSION

Over the years, South African retailers have come under increased pressure to gain PCI DSS (Payment Card Industry Data Security Standards) Compliance. This has resulted in a great deal of confusion, increased complexity within the retailer's environment and has raised concerns around ROI.

Input from banks, PCI assessors, payment processors, hardware vendors and networks suppliers have added to the confusion, resulting in more questions than answers. What is the true value of PCI DSS Compliance? Is it all just a money making machine? Is it worth the time, cost and effort? How long can it be delayed?

These questions are particularly relevant in today's tough economic climate and fiercely competitive retail market.

This beginner's guide aims to assist retailers in understanding the PCI reality and help them navigate through their own PCI Compliance journey.

FIRST THINGS FIRST

The PCI has arrived and is here to stay. PCI standards play a very important role in protecting YOUR customers' sensitive payment data. With security attacks becoming more sophisticated and PCI penalties becoming more severe, retailers can no longer ignore their card payment security obligations to customers. Forbes reports that "A record number of breaches – 1,611 – took place in 2012, a staggering 48% increase from 2011."[1] Recently, a large US supermarket data breach resulted in 2.4 million credit and debit cards being exposed.[2] That means there are now 2.4 million customers who may have less trust in your brand, 2.4 million customers who may opt to shop elsewhere, and of course 2.4 million potentially lost revenue opportunities. Add PCI penalties to the mix and we are looking at a very bleak outlook for any retailer that experiences a security breach.

IT'S A JOURNEY

PCI DSS Compliance is not a one-time event and there is no silver bullet. Compliance is a journey with many challenges, milestones and tangible successes. The objective of this on-going journey is to protect customers' card data, not just today, but in the future, by following the prescribed security standards.

These standards were designed by the PCI Security Standards Council, better known as the PCI SSC. The Council was formed by MasterCard, Visa, American Express, Discover and JCB International in order to develop, manage, educate and build awareness of the PCI Security Standards.

Ecentric Payment Systems was recently invited to join the ***PCI SSC as a Participating Organization.***

1. Forbes, Data Breaches Cost US Billions, Bill Hardekopf, 10 June, 2013.
2. TechNews Daily, Supermarket Data Breach Exposes 2.4 Million Credit Cards, Ben Weitzenkorn, 16 April 2013.

COMPLIANCE LEVELS EXPLAINED

If your business accepts card payments, you need to gain compliance. PCI DSS compliance is required of all retailers that store, process, or transmit bankcard data. The program applies to all payment channels, including retailers (brick-and-mortar), mail order/telephone order, and e-commerce, no matter the size of the business.

The PCI groups retailers into 4 levels to determine compliance requirements. Each of the 5 card brands have similar Merchant Level criteria based on transaction volume.[3] Merchant Levels for Visa are described below.

MERCHANT LEVEL	DESCRIPTION
Level 1	Level 1 Merchants processing over 6 million Visa transactions annually (all channels).
Level 2	Level 2 Merchants processing 1 million to 6 million Visa transactions annually (all channels).
Level 3	Level 3 Merchants processing 20,000 to 1 million Visa e-commerce transactions annually
Level 4	Level 4 Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually.

THE BENEFITS AND LIMITATIONS

PCI DSS applies not only to IT systems and applications, but also to any procedure that involves bank card account data.

Compliance benefits include:

- Reduced risk of a security breach
- Peace of mind for your business
- Customer confidence
- Protection against costly fines

However, compliance cannot protect you from:

- A careless vendor
- New viruses
- An employee intent on abuse (e.g. card skimming)

3. The Full PCI DSS specification can be found on www.pcisecuritystandards.org

THE 12 GOLDEN RULES

PCI DSS is based on 12 security requirements, which have 6 clear control objectives:

BUILD AND MAINTAIN A SECURE NETWORK

Rule 1: Install and maintain a firewall configuration to protect cardholder data.
Rule 2: Don't use vendor-supplied defaults for system passwords and other security parameters.

PROTECT CARDHOLDER DATA

Rule 3: Protect stored cardholder data.
Rule 4: Encrypt transmission of cardholder data across open, public networks.

MAINTAIN VULNERABILITY MANAGEMENT PROGRAM

Rule 5: Use and regularly update anti-virus software.
Rule 6: Develop and maintain secure systems and applications.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Rule 7: Track and monitor all access to network resources and cardholder data.
Rule 8: Assign a unique ID to each person with computer access.
Rule 9: Restrict physical access to cardholder data.

REGULARLY MONITOR AND TEST NETWORKS

Rule 10: Track and monitor all access to network resources and cardholder data.
Rule 11: Regularly test security systems and processes.

MAINTAIN AN INFORMATION SECURITY POLICY

Rule 12: Maintain an information security policy.

Contact Ecentric to learn more about each of these PCI DSS rules.

COMPLIANCE VS. VALIDATION OF COMPLIANCE

All retailers that accept card payments must comply with the Council's security standards by following the 12 rules noted above. These rules apply not only to systems, but also to people and processes within your business.

In addition to complying with PCI standards, retailers need to verify their compliance by meeting the validation requirements defined by each card brand. Validation criteria are grouped according to Merchant Levels.

If your business falls under Level 1, you will need a Qualified Security Assessor (QSA) and an Approved Scan Vendor (AVS) to validate your compliance.

So what exactly are a QSA and AVS? A QSA is a company approved by the PCI SSC to conduct on-site assessments, whilst, an AVS is a company approved by the PCI SSC to conduct external vulnerability scanning services.

*In 2008 Ecentric was the **first processor in South Africa to achieve PCI DSS Level 1 compliance status.** Since then, we have successfully maintained our Level 1 status by completing four consecutive annual PCI audits with the support of **Trustwave**, our QSA.*

The PCI SSC offers a set of Self-Assessment Questionnaires (SAQs) to assist Merchant Levels 2, 3 and 4 in compliance validation. An SAQ is a validation tool intended to assist retailers who are permitted by the payment brands to self-evaluate their compliance. This means your business may not require a QSA and you can perform a Self-Assessment by filling the appropriate SAQ forms and storing them in your records. In addition, you may be required to engage with an AVS for security scans.

Compliance criteria vary based on the card brand. Read more about specific requirements on each card company's website: **MasterCard, Visa, American Express, Discover and JCB International.**

DE-SCOPING PCI DSS

"PCI DSS Compliance can quickly become a monumental task for any business to achieve. Retailers have the power to reduce their PCI burden by handling sensitive payment data in their environment only when absolutely required" advises Mike Scott, Managing Director of Ecentric Payment Systems

There are a number of de-scoping opportunities available to retailers in all their channels, including point-of-sale, e-commerce and m-commerce. Let's explore some of these opportunities.

REMOVE CARD DATA - IF YOU DON'T NEED IT, DON'T STORE IT

The first step to de-scoping is identifying areas where you can remove card data from your environment. Here are a few "do not's" to get you started.

Do not store cardholder data unless it's absolutely necessary.

Do not store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card after authorization.

Do not have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked.

Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones.

Do not locate servers or other payment card system storage devices outside of a locked, fully secured and access-controlled room.

Do not permit any unauthorized people to access stored cardholder data.

TOKENISATION AND POINT-TO-POINT ENCRYPTION, SECURING DATA AT REST AND IN FLIGHT

Point-to-Point Encryption (P2PE) involves the encryption of transmitted data, ensuring no sensitive information is available in the clear. P2PE includes the point between the Pinpad and the POS and between the POS and the processor. This enables retailers to avoid complex security requirements within their environment as all sensitive data in flight is encrypted using international standards.

In addition to protecting data in flight, it is a PCI imperative that all data at rest is protected, preventing fraudsters from breaching systems and stealing sensitive data. The PCI council has proposed tokenisation, a process which creates a unique token for a specific card number. Once created, the token is stored across all systems as a representation of the particular card number. A tokenisation server can be used to generate and validate tokens across multiple participants (Store/Processor/Bank). This standard is currently being defined and agreed upon between transaction participants and the card brands.

The essential steps to secure data in flight and at rest:

1. Ensure that the card data is encrypted on the PED at the time that the card is swiped/ inserted.
2. Create a Unique Identifier by which that card/transaction can be tracked for future queries.
3. Propagate the secured/encrypted data within the transaction lifecycle through each link in the chain, i.e. POS, Switch, and Bank.
4. Ensure that all current routing and processing information is maintained and not compromised between each point in the transaction life cycle.
5. Secure all reporting portals and databases so that sensitive data is fully protected.

THE CARD NUMBER DILEMMA

Retailers are often required to quote customer card numbers when lodging queries with their acquiring bank. This introduces a great risk in the retailer's domain as card numbers propagate in various communication mediums (spread sheets, and word documents in emails, SMSs, etc.) To overcome this problem, South African banks are proposing the use of a UTI (Unique Transaction Indicator) which would be printed on receipts and stored on all systems. The UTI is not a derivation of a card number, nor is it a token (as discussed above). It is merely a mechanism to enable retailers to query transactions without ever needing to quote the actual card number.

NETWORK SEGMENTATION

Network segmentation enables retailers to delineate areas within their environment.

The objectives are:

- Segmentation of areas that contain sensitive data.
- Protection of sensitive data from other parts of a network.
- Separation of test and development environments.
- Prevention of Denial of Service attacks if networks are internet facing.
- Implementation of authentication mechanisms for accessing the network.

HOSTED PAYMENT PAGES

For e-commerce and m-commerce, you can utilise hosted payment pages from a PCI Compliant payment gateway. Hosted payment pages are geared towards online retailers that need to accept online payments without ever having to interact with sensitive card details. Your customers enter their payment information on a secure page hosted by a third party, enabling you to eliminate e-commerce payments from PCI DSS scope.

Contact us to learn more about PCI-DSS and how Ecentric Payment Systems can assist you through your PCI Compliance journey.

WE'D LOVE TO HEAR FROM YOU

GIVE US A CALL

Tel. +27 (0)21 681 9600
Fax. +27 (0)21 686 8398

SEND US AN EMAIL

info@ecentric.co.za

VISIT US

www.ecentric.co.za

Ecentric Payment Systems
Great Westerford Building
240 Main Road
Rondebosch
7700
South Africa

ecentric
PAYMENT SYSTEMS

ECENTRIC PAYMENT SYSTEMS, A LEADING SOUTH AFRICAN PCI DSS LEVEL 1 SERVICE PROVIDER.

Ecentric Payment Systems offers a comprehensive suite of payment services in Southern Africa. These include point of sale integration and transaction processing, EMV certification, reconciliation services, ecommerce and mcommerce solutions, collection and payment services, money transfer systems, gift card issuing, and pre-paid services. For more information, visit **www.ecentric.co.za**

© Copyright 2013 Ecentric Payment Systems | All Rights Reserved