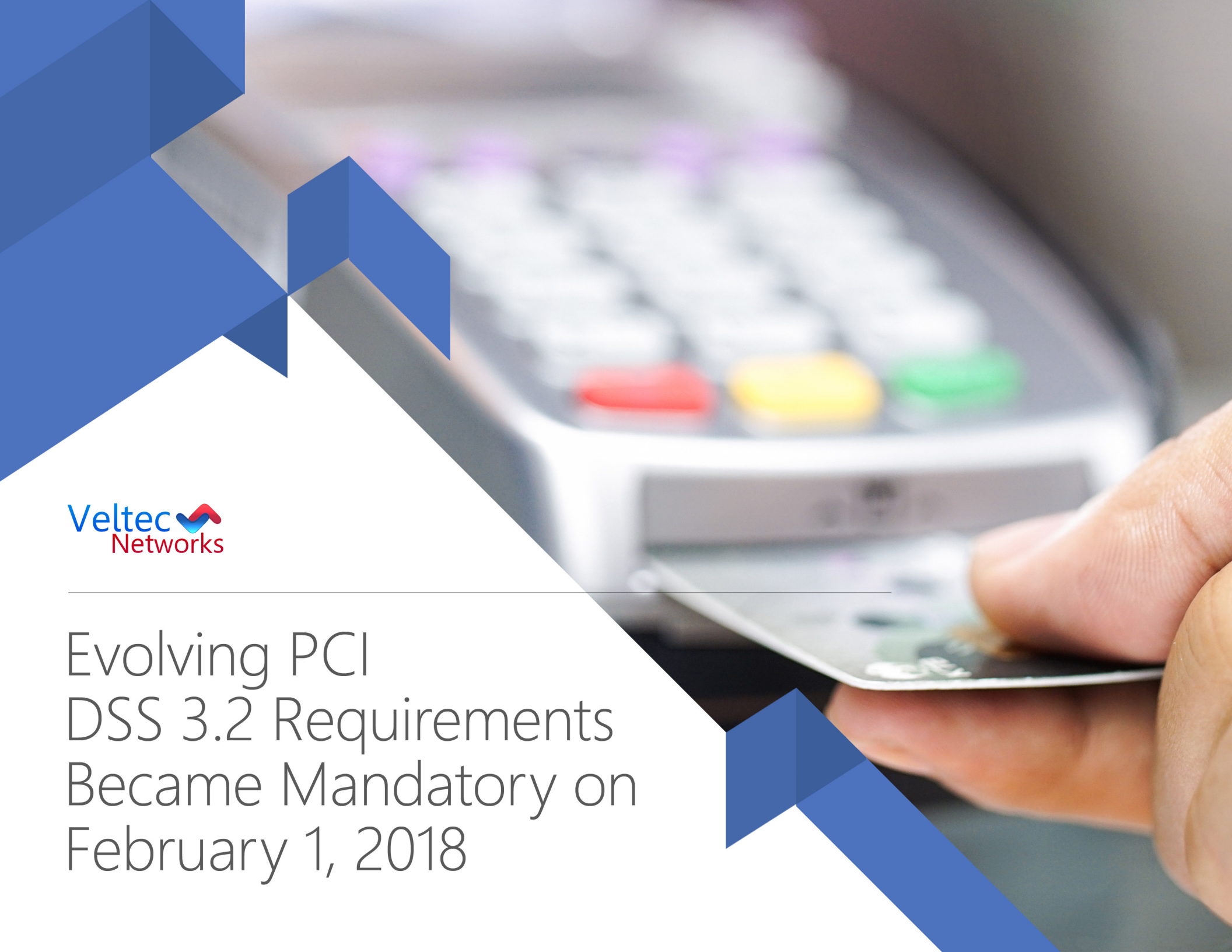


Veltec Networks

Evolving PCI DSS 3.2 Requirements Became Mandatory on February 1, 2018

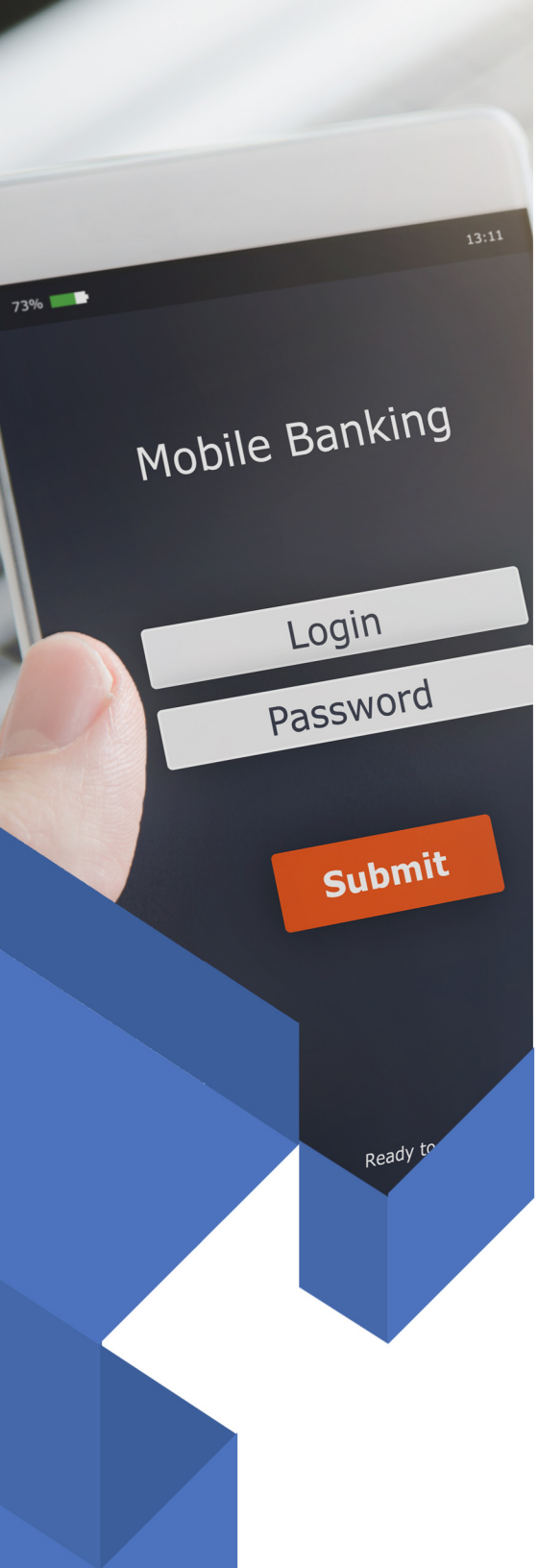
The latest updates from the Payment Card Industry Data Security Standard, known as PCI DSS 3.2, became mandatory on February 1, 2018. This will affect all merchants and service providers who accept credit card payments from Visa, MasterCard, Discover, and American Express. The creators of this iteration believe that PCI DSS 3.2 will provide stronger security measures for consumers against the attacks of cyber-thieves and hackers.

PCI DSS 3.2 affects all merchants who store, process or transmit the sensitive data of cardholders. This highly detailed document contains 12 requirements for safeguarding the data of cardholders. In 2015, PCI DSS v3.0 was used to provide guidelines for merchants regarding compliance. Then, in 2016, PCI DSS v3.1 was released, which clarified many of the requirements of its earlier predecessor PCI DSS v3.0.

Preventing Security Breaches

This annual application- and network-level assessment determines whether devices and systems connected to the Internet possess weaknesses, loopholes, or vulnerabilities that hackers might use to obtain important cardholder information.

The new standards provide comprehensive information designed to reduce risks from cyber intruders. If properly implemented, they will better safeguard the personal banking and account data of customers.



With cyber attacks and digital threats on the rise, the Payment Card Industry works continuously to strengthen their best practices and mandatory requirements. A vital part of this process is the self-assessment process that ensures a company's full compliance with all rules and regulations.

Though this process can be tedious, it is important to carry it out well, correctly and on a regular basis. In fact, penetration testing and vulnerability assessment scans are required every three months. Independent audits may also be required, along with periodic scans. Some of these requirements only pertain to businesses that do a larger volume of cardholder transactions. Scans must be completed by an "approved" scanning company.

The **PCI DSS Self-Assessment Questionnaire** evaluates a service provider or merchant's compliance with those items listed in the PCI Self-Assessment Questionnaire. If weaknesses are identified, the Questionnaire also includes recommendations for bringing the security controls up to full compliance level.

Special Compliance Regulations

Some organizations focus on specific mandates in regards to compliance. For instance, all hospitals, clinics and doctor's offices must comply with current HIPAA standards. For those businesses in one of the many financial industries, the Sarbanes-Oxley Act of 2002 (SOX) provides compliance requirements. With each of these, the goal is to protect consumers against fraud, while also protecting everyone from hackers and cyber thieves.

Below are a few of the updated controls, including new changes to regulations:

Control 3.3 – Changes in Wording

This control will be used by merchants and service providers. Changes in wording to control 3.3 provide greater detail as to how a Credit Card Number or Primary Account Number (PAN) is displayed. Typically, only the first six and last four digits of a credit card number should be displayed. If personnel have a legitimate need to see the entire credit card number, then they are allowed to view it.

Control 3.5.1 - Encryption Architecture Documentation

This control pertains to service providers, and it regulates the use of protocols, algorithms, and keys used in protecting card data. It includes card expiration dates and key strengths. Documentation must include a description of any hardware security modules (HSMs), all protocols, and a description of the cryptographic keys used.

Control 6.4.6 – Verifying PCI DSS Requirements on New and Modified Networks

This control will be used by merchants and service providers. It mandates that all requirements of PCI DSS be implemented in new or modified networks and that these changes be verified. Though this normally is completed by personnel anyway, the new control requires employees to examine records, observe affected systems and interview staff to make sure the applicable PCI DSS requirements were correctly implemented.

Control 8.3.1 – Multiple Authentication Factors for CDEs

In the previous version of PCI DSS, a two-factor authentication process was required. These new standards require "multiple" authentication factors. Though the control does not stipulate how many are required, by changing the terminology from "two-factor" to "multiple", it is clear that at least three types of authentication should be utilized in the cardholder data environment (CDE).

Control 10.8 – Periodic Reporting and Detection of System Failures

This control applies to service providers. It spells out the application process for fault detection, as well as the creation of regular periodic reports. Reports should cover all critical security control systems. These include anti-virus programs, firewalls, FIM, IDS/IPS, logical access controls, physical access controls, segmentation controls, audit logging mechanisms, and others.

Control 10.8.1 - Response to Security Incidents

This control applies to service providers. It mandates that companies have an efficient plan for responding to any breaches or failures. The exact failure and cause (if possible) will be determined and documented. Remedial actions should be taken at once. Managers and directors should determine if any further actions in response to the breach are necessary. New deterrents should be put in place to prevent this type of breach from occurring again.

Control 11.3.4.1 - Tests of Constant Intrusions

This control applies to service providers. It requires that intrusion tests be carried out every six months whenever segmentation of environments are used.

Control 12.11 - Security Policy Reviews

This control applies to service providers only. It requires that all security policies be reviewed every three months to ascertain whether personnel are following the rules and procedures. These reviews should include firewall rules, daily logs, responses to security events, changes to management procedures and any other items regarding system security.

Control 12.11.1 – Maintain Quarterly Review Documentation

This control applies to service providers only, and it stipulates that the regular quarterly review is effectively documented. The person in charge of implementing the PCI DSS compliance program at your company must sign off on these reviews.

Maintaining Public Trust

These are just a few of the new PCI DSS changes that are mandatory by February 1, 2018. All changes were the result of an ongoing effort by the Payment Card Industry Data Security Standard to reduce data breaches and ensure the public's trust. The 3.2 version contains eight evolving requirements, 47 clarifications, and three additional guidance points.

For a full listing of all the new PCI DSS 3.2 requirements, please visit: **PCISecurityStandards.org**.

Veltec Networks

For more information, or assistance establishing a strong cybersecurity posture for your Bay Area business, contact Veltec Networks at (408) 849-4441, Toll Free: (855) 5-VELTEC or email info@veltecnetworks.com.