PAYMENT CARD INDUSTRY DATA SECURITY STANDARD VERSION 3.2 PUBLISHED

The Payment Card Industry Security Standards Council (PCI SSC) has published version 3.2 of the PCI DSS, which provides a baseline of technical and operational requirements designed to protect cardholder data.

Key Updates

Version 3.2 took effect 28 April 2016, incorporating input from global stakeholders. Updates are designed to:
- Accommodate updated migration dates for secure socket layer (SSL) / early transport layer security (TLS).
- Incorporate business-as-usual requirements to ensure continual due care to security controls that protect cardholder data environments.
- Strengthen the security posture for service providers.

Effective Dates for Implementation

The new PCI standard takes effect upon its publication.
- Effective 28 April 2016 through 31 October 2016, organizations may complete PCI DSS validation using versions 3.1 or 3.2. Note: New requirements in version 3.2 should be implemented as best practices until 31 January 2018, after which they will be required.
- Effective 1 November 2016, all organizations must comply with version 3.2 (except new requirements). All new assessments must be performed using version 3.2.
- Effective 1 January 2017, Visa will only accept PCI DSS validations that comply with version 3.2. All version 3.1 validations must be submitted no later than 31 December 2016.
- Effective 1 February 2018, new requirements are no longer best practices and version 3.2 compliance is required.

Visa encourages clients to transition to the updated standards as soon as possible to ensure that data is protected in accordance with the most current security controls.

Additional Resources

The following documents are available at the Documents Library at the PCI SSC website:
- *Payment Card Industry Data Security Standard, Version 3.2*
- *Summary of Changes from PCI DSS Version 3.1 to 3.2*

The following PCI DSS materials have been updated to align with version 3.2 and are available from the PCI SSC website:
- Self-assessment documents
- *Glossary of Terms, Abbreviations, and Acronyms*
- *Prioritized Approach for PCI DSS*
- *Information Supplement: Migrating from SSL and Early TLS*
- Report on Compliance (ROC) templates and Attestation of Compliance (AOC) forms
- Frequently asked questions

For more information on the updated PCI SSC standards, contact your regional Visa risk representative or CISP@visa.com.