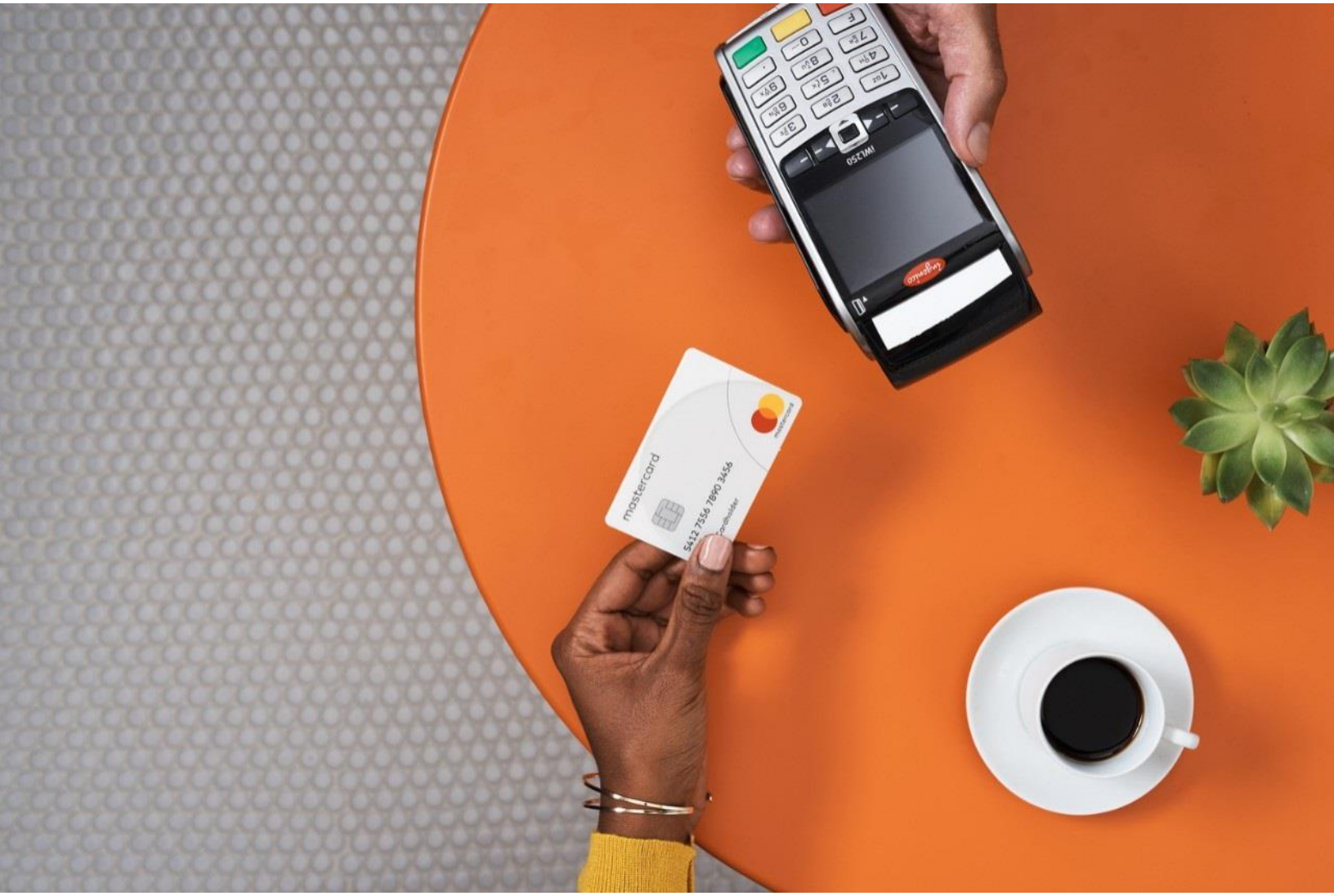


MASTERCARD SITE DATA PROTECTION (SDP) PROGRAM

8-Digit BIN Expansion Mandate and PCI DSS Impact

DECEMBER 2018

mastercard

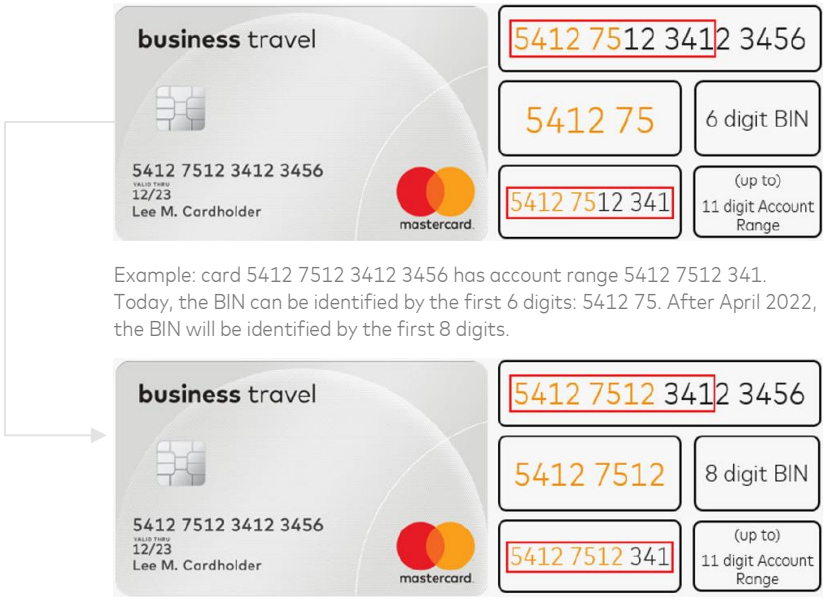
www.mastercard/8-digit BINs

8-DIGIT BIN STANDARD IMPACTS PCI DSS REQ. 3.3 AND 3.4

Background

In the Global Security Bulletin No. 5, 15 May 2017, it was announced that Mastercard will adopt the International Organization for Standardization (ISO) 8-digit BIN standard and will begin assigning 8-digit BINs to issuers by request, effective April 2022. Increasing BIN demand across the entirety of the electronic payments ecosystem has brought about the need for the extension of BINs from the first six digits of a primary account number (PAN) to the first eight digits of a PAN, with no change to PAN length.

To help ensure ecosystem readiness, Mastercard has mandated that all acquirers and their third party processors be able to support 11-digit account ranges and the 8-digit BIN standard by April 2022.



Mastercard Update

Site Data Protection (SDP) Program Standards require that all Level 1-3 merchants and Level 1-2 service providers comply with the Payment Card Industry (PCI) Data Security Standard (DSS) and must validate compliance by completing annual PCI compliance requirements as defined in the in section 10.3.4, "Implementation Schedule," of the Security Rules and Procedures manual.

With the recent BIN expansion mandate, Mastercard's acceptable formats for meeting PCI DSS Requirements 3.3 (mask PAN when displayed) and 3.4 (render PAN unreadable anywhere it is stored) have been updated which could impact an entity's PCI compliance validation.

PCI DSS Impact

The expansion of BINs from 6-digit BINs to 8-digit BINs primarily affects two requirements of the PCI DSS:

- *Requirement 3.3*
  Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN; and

- *Requirement 3.4*
  Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:
  - One-way hashes based on strong cryptography, (hash must be of the entire PAN)
  - Truncation (hashing cannot be used to replace the truncated segment of PAN)
  - Index tokens and pads (pads must be securely stored)
  - Strong cryptography with associated key-management processes and procedures.

MASKING

Req. 3.3—A method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of the PAN when displayed or printed.

TRUNCATION

Req. 3.4—A method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of the PAN when stored in files, databases, etc.

www.mastercard/rules

MASTERCARD SDP STANDARDS

Security Rules and Procedures note that all merchants and service providers that store, process, or transmit cardholder data must validate PCI DSS compliance annually.

©2018 Mastercard. Proprietary. All rights reserved.

While the intent of Requirement 3.3 is to display no more than the "first six and last four digits" of a PAN, an entity will be permitted to display more digits if needed but only with a documented business justification.

For Requirement 3.3, the masking approach should always ensure that only the minimum number of digits is displayed as necessary to perform a specific business function. For example, if only the last four digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last four digits. While the intent of Requirement 3.3 is to display no more than the "first six and last four digits" of a PAN, an entity will be permitted to display more digits if needed but only with a documented business justification.

For Requirements 3.4, the maximum digits of a PAN that can be stored using truncation are "first six and any other four." Mastercard's acceptable truncation format has not changed as a result of the 8-digit BIN expansion mandate. If an entity needs to store more than "first six and any other four," then truncation cannot be used to meet Requirement 3.4 and one of the other three approaches would need to be applied to render the PAN unreadable anywhere it is stored.

Note—PCI DSS Requirement 3.3 relates to protection of the PAN displayed on screens, paper receipts, printouts, etc., and is not to be confused with PCI DSS Requirement 3.4 for protection of PAN when stored in files, databases, etc.

If an entity needs to store more than "first six and any other four," then truncation cannot be used to meet Requirement 3.4 and one of the other three approaches would need to be applied to render the PAN unreadable anywhere it is stored.

Frequently Asked Questions

The following list of PCI Council questions on acceptable formats for masking and truncation of PANs can be found on the PCI Council's website:

What is the difference between masking and truncation?

What are acceptable formats for truncation of primary account numbers?

Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?

Can the full credit card number be displayed within a browser window?

For More Information

For more information on Mastercard's adoption of the ISO 8-digit BIN standard and impacts on an entity's PCI DSS compliance validation, please send an email to: sdp@mastercard.com or BIN_Inquiries@mastercard.com. In addition, the following resources are available to you:

Mastercard

The Mastercard PCI 360 website contains information including white papers and webinars on cardholder data security. This site offers beginner to expert level training curricula suitable for merchants of all sizes and complexity.

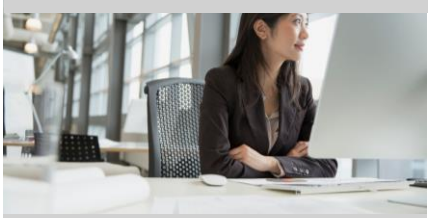
Mastercard PCI 360 Education Portal: www.mastercard.com/pci360
Mastercard Site Data Protection Program Site: www.mastercard.com/sdp

The Payment Card Industry Security Standards Council

The PCI SSC's Document Library includes a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step.

PCI SSC Document Library: www.pcisecuritystandards.org/document_library
PCI SSC Site: www.pcisecuritystandards.org

www.mastercard.com/pci360



For frequently asked questions about the Mastercard SDP Program, such as compliance validation requirements for Level 1-Level 4 merchants and appropriate validation tools merchants can use including SAQs, ASV Scans, and On-site Assessments, download the SDP Program- FAQs document on the PCI 360 website.

©2018 Mastercard. Proprietary. All rights reserved.