# 8-Digit BIN Expansion and PCI Standards

Site Data Protection Program

UPDATED—October 20, 2021

## Important Note

The purpose of this document is to answer Payment Card Industry (PCI) and Site Data Protection (SDP) Program frequently asked questions about the payments' industry migration to 8-digit BINs and provide clarification on the use of Mastercard's allowable truncation format for rendering the full primary account number (PAN) unreadable when stored.

**Key Takeaways:**

- 8-digit BIN expansion does not directly affect compliance with the PCI Data Security Standard (DSS) or SDP Program.
- Mastercard strongly recommends that entities retain the fewest digits of a PAN as possible.
- Mastercard's allowable truncation format is not mandatory.
- Entities are not required to change their current format for truncation as a result of the migration to 8-digit BINs.

### 8-digit BIN Standard

Increasing demand for Bank Identification Numbers (BINs) across the electronic payments ecosystem has created the need for the extension of BINs from the first 6 digits of a PAN to the first 8 digits of a PAN. Emerging payment technologies, such as tokenization, have impacted BIN demand.

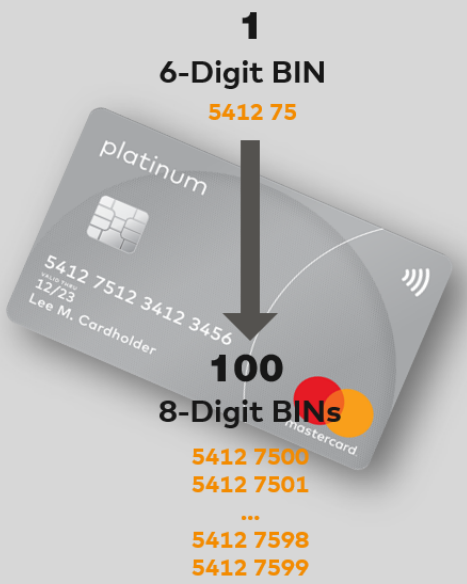
In 2017, Mastercard announced that it would adopt the International Organization for Standardization (ISO) 8-digit BIN standard and begin assigning 8-digit BINs to issuers by request, effective April 2022. To help ensure ecosystem readiness, Mastercard has mandated that all acquirers and their service providers, including processors, support 11-digit account ranges and the 8-digit BIN standard by April 2022.

**What is changing?**

- **BIN length** is expanding from **6 Digits to 8 Digits** as defined by **ISO 7812-2**
- **Acquirers will need to process** the first 8 digits of the PAN to identify the BIN
- **Issuers encouraged, but not required** to adopt 8-digit BINs
- Each 6-digit BIN will encompass 100 8-digit BINs
- BIN Sharing rules will apply to 8-digit BINs, Issuers will be allowed to have 8-digit Consumer, Commercial, Credit or Debit BINs with the same first 6 digits
- **Acquirer Only BINs will be renamed Acquirer Reference ID,** will remain 6 digits

**What is not changing?**

- PAN length will remain the same
- Mastercard account ranges will remain up to the first 11 digits of a PAN (incl. BIN)
- Customers will continue to use account ranges to maximize efficient use of BINs; to further segment a portfolio by product, interchange, geography
- BIN tables will continue to show ranges as they do today



**PCI Data Security Standard**

There are two PCI DSS requirements that may be affected when considering 8-digit BINs:

- *Requirement 3.3*
  Mask PAN when displayed (the first 6, last 4 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 6/last 4 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.

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 6 and last 4 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 8, any other 4."

**Mastercard strongly recommends that entities retain the fewest digits possible. Mastercard's allowable truncation format is not mandatory. Entities are not required to change their current format, if utilized, for the purposes of compliance with the PCI DSS or SDP Program.**

If an entity needs to store more than "first 8, any other 4," 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.*

PCI DSS

MASKING

Req. 3.3—Mask PAN when displayed (the first 6, last 4 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 6/last 4 digits of the PAN.

TRUNCATION

Req. 3.4— Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs). The maximum digits of a PAN that can be stored using truncation are "first 8, any other 4."

IMPORTANT

Mastercard strongly recommends that entities retain the fewest digits possible. Mastercard's truncation format is not mandatory. Entities are not required to change their current format, if utilized, for the purposes of compliance with the PCI DSS or SDP Program.

**PCI DSS Compliance Validation Exemption Program**

Merchants concerned with complying with the PCI DSS as a result of the payments' industry migration to 8-digit BINs can benefit from participating in the Mastercard PCI DSS Compliance Validation Exemption Program (Exemption Program).

The Exemption Program is an optional, global program within the SDP Program that eliminates the requirement for merchants using secure payment technologies to validate PCI DSS compliance annually. The program incentivizes both card present and card not present merchant participation. Only merchants using EMV chip technology, PCI point-to-point encryption (P2PE) solutions or EMV Payment Tokenization may participate in the program.

Interested merchants should contact their acquiring bank who manages their PCI DSS compliance. The acquirer will then validate to Mastercard that all Exemption Program qualification requirements have been met as defined in 2.2.4 Mastercard Cybersecurity Incentive Program (CSIP) of the *Security Rules and Procedures*. As a best practice, but not required, Mastercard recommends merchants participating in the Exemption Program validate compliance with the PCI DSS within twelve months of entering the program.

PCI DSS EXEMPTION

INCENTIVE

The Exemption Program can benefit eligible merchants using secure technologies such as EMV chip, point-to-point encryption (P2PE) or EMV payment tokenization by eliminating the requirement to annually validate PCI DSS compliance.

## Frequently Asked Questions

The following PCI questions are designed to assist acquirers, service providers, including processors, and merchants on the 8-digit BIN expansion.

### How can an entity distinguish a 6-digit BIN from an 8-digit BIN?

As used solely for the purposes of the SDP Program and compliance with the PCI DSS, entities should proceed under the assumption that all Mastercard PANs are 8-digit BINs. This assumption is designed to simplify the PCI DSS assessment process to meet SDP Standards and has no bearing on any application other than PCI DSS validation.

### Are entities required to use truncation to render the PAN unreadable?

No.

### Are entities required to truncate the PAN to no more than "first 8, any other 4"?

No. Mastercard's allowable truncation format, "first 8, any other 4", is not mandatory. Mastercard strongly recommends entities retain the fewest digits of the PAN as possible. For example, if a PCI DSS compliant merchant is currently using "first 6, any other 4" to truncate PANs, that merchant is not required to make any changes to their current format for truncation as a result of the migration to 8-digit BINs and PCI DSS compliance.

### What can entities do to validate their compliance with the PCI DSS if they decide to make changes to their payment environment as a result of the migration to 8-digit BINs?

Mastercard recommends that entities engage a PCI Security Standards Council (PCI SSC) Qualified Security Assessor (QSA) if they decide to make changes to their payment environment as a result of the migration to 8-digit BINs.

### How can merchants apply for the Exemption Program which eliminates the requirement to annually validate PCI DSS compliance?

Merchants that meet the qualification criteria for the Exemption Program should first contact their acquiring bank who manages their PCI DSS compliance. It is the responsibility of the acquirer to validate that the merchant meets all program requirements and contacts Mastercard at sdp@mastercard.com. There is no application form or fee to enter in the program.

The following list of PCI SSC questions related to the 8-digit BIN migration and published 8-digit BIN blogs can be found on the PCI SSC website at www.pcisecuritystandards.org/faqs and www.blog.pcisecuritystandards.org/topic/8-digit-bin.

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?

How can an entity meet PCI DSS requirements for PAN masking and truncation if it has migrated to 8-digit BINs?

## For More Information

For more information on Mastercard's adoption of the ISO 8-digit BIN standard, please send an email to BIN_Inquiries@mastercard.com.

For more information on Mastercard's SDP Program and 8-digit BIN considerations on an entity's PCI DSS compliance validation, please send an email to sdp@mastercard.com. In addition, the following resources are available to you:

### Mastercard

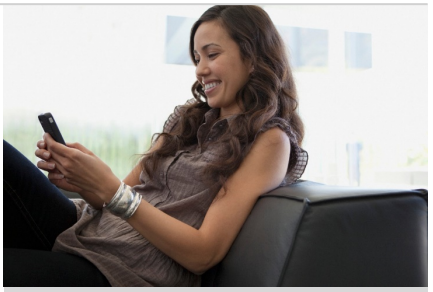
The Mastercard PCI 360 website helps educate customers, merchants and service providers with the tools and resources they need to meet Mastercard SDP Program requirements.

*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



SDP PROGRAM

For commonly asked questions about the SDP Program, such as compliance validation requirements for merchants and service providers, including appropriate validation tools, download Mastercard Cybersecurity Standards and Programs FAQs.