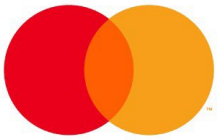

Virtual Card Numbers and SDP Compliance

Frequently Asked Questions

30 November 2023

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third-party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

Document Purpose

The purpose of this document is to answer commonly asked questions about virtual card numbers (VCNs) as they relate to Site Data Protection Program Standards governed under Mastercard Cybersecurity Standards and Programs.

Reference Document

The ***Security Rules and Procedures***—*Chapter 2 Cybersecurity Standards and Programs*—is available on Mastercard Connect™ for further references.

Virtual Card Numbers and SDP Compliance—Frequently Asked Questions

Q: What is a virtual account?

A virtual account is a Mastercard account issued without a physical card or access device. A virtual account cannot be electronically read.

Q: What is a Mastercard account?

A Mastercard account is any type of account (credit, debit, prepaid, commercial, etc.) identified as a Mastercard account with a primary account number (PAN) that begins with a Bank Identification Number (BIN) in the range of 222100 to 272099 or 510000 to 559999.

Q. How does the Payment Card Industry Data Security Standard (PCI DSS) define PAN?

PCI DSS defines PAN as a unique payment card number that identifies the issuer and the cardholder account. The PAN is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the cardholder data environment (CDE), they must be protected in accordance with applicable PCI DSS requirements.

Q: Is it required that a virtual Mastercard account be assigned a Card Validation Code 2 (CVC 2) value and a card expiration date?

Yes. A virtual Mastercard account must be assigned a CVC 2 value and a card expiration date.

Q: Can a virtual account be issued for multiple uses?

Yes. A virtual account issued for multiple uses is called a Multiple Use-Virtual Card Number (MU-VCN).

Q: Can a virtual account be issued for single use (one-time only)?

Yes. A virtual account issued for single use (one-time only) is called a Single Use-Virtual Card Number (SU-VCN).

Q: When can a SU-VCN be considered out of scope for PCI DSS?

Three primary conditions must be met for a SU-VCN to be considered out of scope for the PCI DSS:

- It must be shown that the SU-VCN becomes inactive/disabled after only one authorization creating a single clearing record (additional clearing records created by refunds or other exception processing related to the original SU-VCN authorization do not bring the original SU-VCN transaction into PCI scope); **AND**
- Must be met by a technological control that cannot be circumvented; **AND**
- The systems that store, process, or transmit the SU-VCN do not also store, process, or transmit other in scope PANs.

NOTE—Mastercard recommends that entities consult with a PCI Security Standards Council (PCI SSC)-approved Qualified Security Assessor (QSA) to understand whether or not SU-VCNs (one-time use payment cards) are considered in scope for PCI DSS. QSA companies have been qualified by the PCI SSC to validate an entity's adherence to PCI DSS and therefore, are in a better position to assess an entity's existing controls.

Q: Why does Mastercard consider properly segmented SU-VCNs to be out of scope for PCI DSS?

As the SU-VCN becomes inactive/disabled after only one authorization creating a single clearing record, the virtual PAN data cannot be reused for fraudulent activities within the payment ecosystem.

Q: When can a MU-VCN be considered out of scope for PCI DSS?

Three primary conditions must be met for a MU-VCN to be considered out of scope for the PCI DSS:

- It must be shown that the MU-VCN exclusively uses dynamic Card Validation Code 2 (CVC 2); **AND**
- Failure of CVC 2 validation during authorization must always result in a decline; **AND**
- The systems that store, process, or transmit the MU-VCN do not also store, process, or transmit other in scope PANs.

NOTE—Mastercard recommends that entities consult with a PCI Security Standards Council (PCI SSC)-approved Qualified Security Assessor (QSA) to understand whether or not MU-VCNs are considered in scope for PCI DSS. QSA companies have been qualified by the PCI SSC to validate an entity's adherence to PCI DSS and therefore, are in a better position to assess an entity's existing controls.

Q: Can a MU-VCN with static CVC 2 be considered out of scope for PCI DSS?

No. MU-VCNs that use static CVC 2 are always in scope for the PCI DSS.

Q: My entity is using a Mastercard product or solution that offers VCN capabilities. Will Mastercard assist with the security and PCI DSS scoping considerations for those VCNs?

Yes. If an entity is using a Mastercard product or solution that offers VCN capabilities (e.g., Mastercard inControl™), Mastercard can provide guidance on the security and PCI DSS scoping considerations for those VCNs.

Q: My entity is using a third-party product or solution that offers VCN capabilities. Will Mastercard assist with the security and PCI DSS scoping considerations for those VCNs?

No. If an entity is using a third-party product or solution that offers VCN capabilities, we recommend contacting that third-party product or solution provider directly for advice and guidance on how to utilize their product or service. Additionally, Mastercard recommends that entities consult with a QSA to understand whether VCNs are considered in scope for PCI DSS. QSA companies have been qualified by the PCI SSC to validate an entity's adherence to PCI DSS and therefore, are in a better position to assess an entity's existing controls.

Q: What is tokenization?

Tokenization is the process by which a Mastercard token replaces an account PAN.

Q: Is a PAN tokenized for use on a mobile payment device considered a virtual account?

No. A PAN tokenized for use on a mobile payment device is not considered a virtual account.

Q: Does Mastercard consider the use of tokens generated in accordance with the EMV Payment Tokenization Specification in scope for PCI DSS?

No. Mastercard does not consider the use of tokens generated in accordance with the EMV Payment Tokenization Specification in scope for PCI DSS.

Q: Does Mastercard consider a SU-VCN to be an issuer token?

Yes. A SU-VCN is considered to be an issuer token.

Q: Is an issuer token the same as an EMV Payment Token?

No. An issuer token is not the same as an EMV Payment Token.

Q: How can merchants using secure technologies such as EMV Payment Tokenization eliminate the requirement to annually validate PCI DSS compliance?

Merchants using EMV Payment Tokenization can benefit from participating in the Mastercard PCI DSS Compliance Validation Exemption Program (Exemption Program), an optional, global program which eliminates the requirement for merchants to annually validate their PCI DSS compliance to Mastercard.

Q: How can eligible merchants participate in the Exemption Program?

To participate in the Exemption Program, eligible merchants must not store sensitive authentication data (SAD), must have an established (including annual testing) Account Data Compromise (ADC) Event incident response plan in accordance with PCI DSS requirements and must meet one of the following requirements:

a. At least 75 percent of the merchant's annual total acquired Mastercard and Maestro transaction count is processed through Hybrid POS Terminals; **OR**
b. Implemented a validated PCI point-to-point encryption (P2PE) solution listed on the PCI SSC website; **OR**
c. At least 75 percent of the merchant's annual total acquired Mastercard and Maestro Transaction count is processed using EMV Payment Tokens from Token Service Providers (TSP) compliant with Mastercard TSP Standards.

Q: Where can I find additional information on Mastercard rules relating to the issuance of virtual accounts?

Additional information on Mastercard rules relating to the issuance of virtual accounts can be found in section 6.7, "Virtual Accounts", of the *Mastercard Rules*.

Q: Where can I find Mastercard SDP Standards and who can I contact for more information on VCNs and SDP compliance?

Mastercard SDP Standards can be found in section 2.2, "Mastercard Site Data Protection (SDP) Program", of the *Security Rules and Procedures*.

Entities with questions about VCNs and SDP compliance should contact the SDP Team at sdp@mastercard.com.