Visa Business News

Data Security 11 June 2020

Expanded Position on PCI DSS Applicability for Virtual Visa Accounts

Global | *Acquirers, Issuers, Processors, Agents*

Visa, Interlink, Plus Networks; V PAY; Europe Processing

> **Overview:** Visa is providing updated information on the applicability of the Payment Card Industry Data Security Standard (PCI DSS) requirements for virtual Visa accounts.

As the use cases for virtual Visa accounts increase, it is necessary to expand on how data security requirements apply to virtual Visa account data handled by industry stakeholders.

Visa requires organizations that store, transmit or process Visa account data to protect that data in accordance with the Payment Card Industry Data Security Standard (PCI DSS). Visa manages its Account Information Security Program to define the compliance and validation requirements for various stakeholders with regard to PCI DSS.

However, the program does not include explicit information on how these security requirements apply to virtual Visa account data. This updated guidance is designed to help improve stakeholder understanding of how virtual Visa account data must be protected.

The following points define Visa's updated position on the applicability of PCI DSS to virtual Visa accounts:

- Tokens generated in accordance with the *EMVCo Payment Tokenisation Specification* are not considered to be Visa account data and are not in scope for PCI DSS protection requirements.
- Visa considers single-use virtual Visa account numbers and multi-use virtual Visa account numbers with Dynamic Card Verification Value 2 (dCVV2) out of scope for PCI DSS protection requirements based on the low risk of fraud associated with the account type.
- All other Visa primary account numbers (PANs) must be protected in accordance with PCI DSS.
- In environments where a Visa PAN (i.e., stored credential) is maintained and not segmented from other virtual Visa account types, PCI DSS requirements are applicable across the full environment.

Note that these positions reflect Visa's requirements for the protection of virtual Visa account data and are not representative of a position from the PCI Security Standards Council or any independent security assessor. Clients must ensure that all virtual accounts issued meet the requirements established in the Visa Rules for this account type (ID#: 0001643). Visa will continue to monitor fraud and compromise trends and may adjust data security requirements in the future as necessary to protect the payment system.

Although some virtual Visa accounts may be out of scope for PCI DSS applicability, Visa strongly recommends that stakeholders take steps to protect virtual Visa account information against fraudulent activity or data breach loss. The positions noted above result in no change for a client's responsibility to comply with the Visa Rules, including but not limited to responsibilities associated with the loss or suspected loss of Visa account information.

For More Information

Merchants and third party agents should contact their acquirer.