Visa Business News

Data Security

7 January 2021

Shared Data Security Responsibilities When Using a Cloud Service Provider

Global | *Acquirers, Issuers, Processors, Agents*

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

Overview: To ensure a secure and compliant payment environment, organizations using cloud service providers must understand the risks and responsibilities under the Payment Card Industry Data Security Standard (PCI DSS). Visa reminds clients, including sponsored agents and merchants, to list all facilities that the PCI DSS assessment covers (retail outlets, corporate offices, data centers, call centers, etc.) in the PCI Attestation of Compliance (AOC) and/or Report on Compliance (ROC) documents.

Visa clients, merchants and agents that outsource payment-related services to cloud service providers must understand the joint responsibilities for the security of applications and Visa account data hosted in the cloud. In April 2018, the PCI SSC published version 3 of its Information Supplement document, *PCI SSC Cloud Computing Guidelines*, which provides overall guidance on the use of cloud technologies and considerations for maintaining security controls in cloud environments. To better understand the PCI DSS considerations for the overall environment, Visa encourages clients, as well as merchants and agents, to refer to this document when planning to use cloud service providers.

Data breaches and unauthorized access to cardholder information continue to be a threat. However, implementation errors and system weaknesses that attribute to security incidents may be averted when the customer is actively engaged. With cloud infrastructure gaining popularity, it is important for customers to understand the roles that both they and the service provider play in the protection of Visa account data. For example, cloud service providers typically maintain the physical security of the infrastructure, but customers may be responsible for protecting the way the information is accessed. Because each cloud service provider may use a different approach to service offerings and data protection mechanisms, customers must be aware which party is managing data security.

Managing Responsibilities

Understand overall risk

When moving payment-related activities to the cloud, an organization must maintain a clear view on the scope of the cloud service provider's involvement with regard to storing, processing or transmitting Visa account data. A service provider may be engaged for services that differ from customer to customer. Hence, scoping is critical for understanding the overall risk. While the customer may outsource the maintenance of some controls to the cloud service provider, the overall responsibility for securing Visa account data remains with the customer.

Written agreements, policies and procedures

To accurately define roles and responsibilities, customers must be aware of PCI DSS responsibilities that are shared across services and system components in order to ensure coverage in those areas. For example, a cloud service provider may be responsible for managing a subset of the controls and only validate to the applicable PCI DSS requirements. To avoid ambiguity and disputes, roles and responsibilities of each party must be assigned and agreed upon in writing. Policies and procedures must support the agreed-upon position.

Compliance Validation

The PCI DSS security requirements apply to all system components included in, or connected to, the cardholder data environment (CDE). When an entity's CDE is located in the cloud, the scope of PCI DSS applies not only to the cloud systems, but also to the systems that may reside on the customer's premise which are connected to the CDE for access or management of the data. It is critically important that an evaluation by a PCI Qualified Security Assessor (QSA) or a knowledgeable staff member is performed to adequately determine PCI DSS scope.

Visa reminds clients, including sponsored agents and merchants, to list all facilities the PCI DSS assessment covers (retail outlets, corporate offices, data centers, call centers, etc.) in the PCI Attestation of Compliance (AOC) and/or Report on Compliance (ROC) documents. In addition, assigning responsibility to a cloud service provider for managing security controls does not exempt the customer from overall responsibility to secure Visa account data in accordance with PCI DSS. To document PCI DSS compliance, customers may provide an AOC for their own environment along with an AOC from the cloud service provider demonstrating how data is protected in both environments. Together, both AOCs should cover the entire CDE and associated PCI DSS responsibilities. Visa clients may be subject to liability for losses resulting from an account data compromise of their environment or that of sponsored merchants and agents.

Third Party Compliance Status

A third party that provides a service that is in scope of an organization's PCI DSS environment may impact the organization's compliance. Note that using a PCI DSS-compliant cloud service provider does not automatically result in an organization's own PCI DSS compliance. Specifically:

- If a cloud service provider is PCI DSS compliant, this does not mean that its downstream customers are compliant.
- If one or more of a cloud service provider's customers is PCI DSS compliant, this does not mean that the cloud service provider is compliant.
- If a cloud service provider and the customer are PCI DSS compliant, this does not mean that any other downstream customers are compliant.

Each organization and configuration for the use of cloud services providers is unique, and shared responsibilities for meeting PCI DSS controls may differ. Therefore, organizations using cloud service providers must understand the risks and responsibilities to ensure a secure and compliant environment.

For More Information

Merchants and third party agents should contact their acquirer.