

Why you must be in compliance with PCI

Regulations

The Operating Regulations for the payment networks govern the activities of member financial institutions (Acquirers) and, by extension, merchants and service providers as participants in the payment systems.

Acquirers must comply with PCI and are responsible for ensuring the compliance of their merchants, and merchants' service providers. Acquirers must include a PCI compliance provision in all contracts with merchants and agents. Specific compliance requirements and validation criteria can be found at www.pcisecuritystandards.org.

Compliance Fines

If a merchant or service provider does not comply with the security requirements or fails to rectify a security issue, Visa and MasterCard may:

- Fine the responsible party
- Impose restrictions on the merchant or its agent

The Acquirer may waive fines in the event of a data compromise if there is no evidence of non-compliance with PCI DSS. To prevent fines a merchant, or service provider must maintain full compliance at all times, including at the time of breach as demonstrated during a forensic investigation. Additionally, a merchant must demonstrate that prior to the compromise the compromised entity had already met the compliance validation requirements.