BARCLAYS

External Supplier Control Obligations

Payment Card Industry Data Security Standard (PCI DSS)

Version 13.0 September 2023

Control Title	Description	Why this is important
Attain Card Data Compliance	The Supplier shall comply with the current versions of the Payment Card Industry Data Security Standards as issued by the Payment Security Standards Council, such as PCI DSS, PA-DSS, PCI-P2PE, PCI-PTS, PCI Card Production.	Protect Cardholder Data: The recognised standard to achieving this is PCI DSS and is a global industry regulatory requirement. PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data.
Supplier & Merchant Attestation	Supplier must provide an Attestation of Compliance for Onsite Assessments (AoC), or where applicable, a Self-Assessment Questionnaire (SAQ), applicable to the scope of the services provided to Barclays, pre-contract and annually thereafter. This must be in accordance with PCI DSS requirements - see **www.pcisecuritystandards.org/** If there are questions raised upon review of the AoC such as with regards to the scope of services, description of the environment or the supplier's PCI compliance, the underlying Report on Compliance (RoC), may be requested and reviewed for further information. A redacted RoC may be acceptable if it confirms the scope of PCI certification applies to the scope of services provided, or other questions raised by Barclays after reviewing the AoC. Supplier must notify Barclays upon becoming non-compliant i.e. as soon as possible and no later than 30 days from the date of expiry of the validation documents.	Evidence that a supplier or merchant has attained the relevant Card Data compliance for the scope of the services provided to Barclays and adhered to the requirements. Evidence that the supplier attestation AoC / RoC or SAQ relates to the service provided. If Barclays are using any supplier or merchant who are non-compliant with PCI DSS they will be required to contact the Visa Europe Third Party Risk team (agentcompliance@visa.com) via email to confirm the supplier or merchant are implementing PCI DSS and has provided Visa Europe with a PCI DSS status plan (using the Visa Europe template) for Visa Europe's review and approval.

Supplier acknowledgement	The supplier must acknowledge in writing to Barclays pre-contract that they are responsible for the security of cardholder data for the following services that they possess / store / process / transmit, or that could impact the security of Barclays customer's cardholder data environment e.g. security services (such as authentication servers), web hosting etc. Any changes to the service provided must be acknowledged in writing to Barclays prior to change implementation.	**From PCI DSS v3.2.1** **Testing procedure for 12.8.2:** Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: In conjunction with Requirement 12.9, this requirement for written agreements between organizations and service provides is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service. **Guidance for 12.8.2:** The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The service provider's internal policies and procedures related to their customer engagement process and any templates used for written agreements should include provision of an applicable PCI DSS acknowledgement to their customers. The method by which the service provider provides written acknowledgment should be agreed between the provider and their customers.

Use of Third-Party Service Providers / Outsourcing

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

Parties should clearly identify the services and system components which are included in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. For example, a managed hosting provider should clearly define which of their IP addresses are scanned as part of their quarterly vulnerability scan process and which IP addresses are their customer's responsibility to include in their own quarterly scans.

Service providers are responsible for demonstrating their PCI DSS compliance, and may be required to do so by the payment brands. Service providers should contact their acquirer and/or payment brand to determine the appropriate compliance validation.

There are two options for third-party service providers to validate compliance:

1) **Annual assessment**: Service providers can undergo an annual PCI DSS assessment(s) on their own and provide evidence to their customers to demonstrate their compliance; or
2) **Multiple, on-demand assessments**: If they do not undergo their own annual PCI DSS assessments, service providers must undergo assessments upon request of their customers and/or participate in each of their customer's PCI DSS reviews, with the results of each review provided to the respective customer(s)

If the third party undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The specific type of evidence provided by the service provider to their customers will depend on the agreements/contracts in place between those parties. For example, providing the AOC and/or relevant sections of the service provider's ROC (redacted to protect any confidential information) could help provide all or some of the information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data. *Refer to Requirement 12.8 in this document for details.*