Service Provider Categories and PCI

	All Service Providers registered with Mastercard that store, process, or transmit cardholder data must validate compliance annually.										
Service Provider[1]	TPP	DSE	PF	SDWO	DASP	TSP	TS	AML	3-DSSP	ISP	MPG
Category	Third Party Processor (TPP)	Data Storage Entity (DSE)	Payment Facilitator (PF)	Staged Digital Wallet Operator (SDWO)	Digital Activity Service Provider (DASP)	Token Service Provider (TSP)	Terminal Servicer (TS)	AML/Sanctions Service Provider (AML)	3-D Secure Service Provider (3-DSSP)	Installment Service Provider (ISP)	Merchant Payment Gateway (MPG)
Program Service (as defined in the Mastercard Rules manual)	• Provides service support for mobile remote payment functionality, which is initiated by an enrolled cardholder from a cardholder-controlled mobile phone registered with the issuer, and used for entry of a cardholder's PIN or mobile specific credentials • Authorization services, including but not limited to authorization routing, switching services, voice authorization, and call referral processing • Clearing file preparation and submission • Settlement processing (excluding possession, ownership, or control of settlement funds, which is not permitted) • Cardholder, merchant, and/or account holder statement preparation affording access to account data, transaction data, Payment Transfer Activity (PTA) account data, and/or PTA transaction data • Cardholder and/or account holder customer service affording access to account data, transaction data, PTA account data, and/or PTA transaction data • Integration with the applicable Mastercard systems for the purpose of origination or reception of PTA transaction	• Merchant website hosting or other service involving the computer-based storage of account, transaction, PTA account, or PTA transaction data • External hosting or provision of payment applications, such as website shopping carts • Encryption key loading • Any other service determined by Mastercard in its sole discretion to be DSE Program Service	• Enters into a sponsored merchant agreement as an agent of an acquirer with each merchant, including as required in rule 7.8.1 of the Mastercard Rules manual) • Submit to the acquirer records of valid transactions submitted to the Payment Facilitator by the sponsored merchants • Timely pay submerchants for transactions submitted to the Payment Facilitator by the sponsored merchants	• Operates and offers to consumers a Staged Digital Wallet • A Payment Facilitator cannot be a Payment Facilitator for a Staged Digital Wallet.	• Provisioning and token requestor services with Mastercard Digital Enablement Service (MDES) on behalf of an issuer • Provisioning services with MDES on behalf of a token requestor • Any other service specified by Mastercard in its sole discretion from time to time to be DASP Program Service	• Token generation and issuance • Cardholder or account holder authentication and token activation • Any other service specified by Mastercard in its sole discretion from time to time to be TSP Program Service	• Terminal maintenance and support • Technology deployment allowing any method of terminal transaction, including a transaction using a mobile wallet application • Terminal software system operation • Services to support payment terminal compliance relating to the Payment Card Industry Data Security Standard (PCI DSS) • Any other service determined by Mastercard in its sole discretion to be TS Program Service	• AML compliance, including but not limited to know your customer (KYC), customer due diligence (CDD)/ enhanced due diligence (EDD), and AML transaction monitoring • Sanctions/watchlist screening activities	• Operates a 3-D Secure Server (3-DSS) system that facilitates communication, via the EMV 3- D Secure specification, to initiate cardholder authentication under the Mastercard Identity Check Program rules • Operates an Access Control Server (ACS) system that verifies, via the EMV 3-D Secure specification, whether authentication is available for a card number and device type, and authenticates specific cardholders under the Mastercard Identity Check Program rules	• Enters into an installment lending agreement with an end user that governs the terms of repayment of installment debt by the end user for the purchase of goods and services • Distributes to an end user an account for purposes of completing the payment stage of a transaction between the end user and a retailer covered by the installment lending agreement • Submits to the issuer records of valid transactions conducted pursuant to the Program Service agreement • Provides an installment technology platform hosting the installment lending account and/or performs installment account transactional management services to issuers which may include end user customer service, installment lending authorization services, installment clearing services, installment settlement processing, installment account statement preparation, installment dispute management, and installment fraud screening • Any other service determined by Mastercard in its sole discretion to be Installment Program Service	• Provides technology that captures and sends payment transaction data to an acquirer on behalf of a merchant, whether in a card-present environment or in a card-not-present environment • Acts as the interface between an ecommerce merchant location (e.g., website or mobile app) and the merchant's acquirer

Service Provider Categories and PCI

	All Service Providers registered with Mastercard that store, process, or transmit cardholder data must validate compliance annually.										
Service Provider[1]	TPP	DSE	PF	SDWO	DASP	TSP	TS	AML	3-DSSP	ISP	MPG
	• Fraud control and risk monitoring, including but not limited to fraud screening and fraud scoring services • Chargeback processing for acquirers or issuers • Chargeback processing for merchants or submerchants • Any other service determined by Mastercard in its sole discretion to be TPP Program Service										
Must be registered with Mastercard	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Must validate compliance with the PCI DSS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	PCI 3DS Core Security Standard[2]	Yes	Yes
Site Data Protection (SDP) Program Level[3]	Level 1	Level 1 if DSE has more than 300,000 total combined Mastercard and Maestro transactions annually Level 2 if DSE has 300,000 or less total combined Mastercard and Maestro transactions annually	Level 1 if PF has more than 300,000 total combined Mastercard and Maestro transactions annually Level 2 if PF has 300,000 or less total combined Mastercard and Maestro transactions annually	Level 1	Level 1	Level 1	Level 2	Level 1	Level 1	Level 1	Level 1
Annual PCI DSS assessment resulting in a Report on Compliance (ROC) conducted by a Qualified Security Assessor (QSA)	Yes	Level 1 DSE: Yes Level 2 DSE: Highly Recommended	Level 1 PF: Yes Level 2 PF: Highly Recommended	Yes	Yes	Yes	Highly Recommended	Yes	PCI 3DS Core Security Standard: 3DS Assessor	Yes	Yes
Annual PCI DSS Self-Assessment Questionnaire (SAQ) D-Service Provider	N/A	Level 2 DSE: Yes[4]	Level 2 PF: Yes	N/A	N/A	N/A	Yes[5]	N/A	N/A	N/A	N/A
Annual PCI Attestation of Compliance (AOC) submission to Mastercard	**Yes** - Send PCI AOC to pcireports@mastercard.com after initial registration with the Mastercard Service Provider Registration Team and every year thereafter. If a registered Service Provider is not yet compliant, the PCI Action Plan indicating compliance within twelve (12) months is required to be completed and submitted for review.										

Service Provider Categories and PCI

[1] Service Provider classifications (for example, TPP, DSE, PF, SDWO, DASP, TSP, TS, AML, 3-DSSP, ISP, or MPG) is determined by the Service Provider Registration Team. Service Provider registrations will not be deemed complete until the Service Provider validates compliance with the Mastercard SDP Program.

[2] A Service Provider that performs or provides 3DS functions as defined in the EMV® 3-D Secure Protocol and Core Functions Specification must validate compliance with the PCI 3DS Core Security Standard.

[3] A Level 2 Service Provider that has a confirmed account data compromise (ADC) Event will be automatically reclassified to become an SDP Level 1 Service Provider. PCI compliance validation requirements for Level 1 Service Providers will then apply.

[4] As an alternative to validating compliance with the PCI DSS, a DSE qualifying as a Level 2 Service Provider may submit a PCI PIN Security Requirements AOC from a PCI Security Standards Council (PCI SSC)-approved Qualified PIN Assessor (QPA), provided that the DSE does not perform services involving the storage, transmission, or processing of account, cardholder, or transaction data.

[5] As an alternative to validating compliance with an annual SAQ D-Service Provider, a TS may submit a Terminal Servicer Qualified Integrator and Reseller (QIR) Participation Validation Form, provided that the TS does not store, transmit, or process account, cardholder, or transaction data, but has access to a merchant's cardholder data environment. See Terminal Servicers and SDP Compliance FAQs for more on eligibility requirements.

Important Note
To be listed on The Mastercard SDP Compliant Registered Service Provider List, updated monthly, a Service Provider must have been registered by one or more Mastercard customers and have submitted a fully executed copy of their PCI AOC by a QSA reflecting validation of PCI compliance.

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.