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]	ISO	TPP	DSE	PF	SDWO	DASP	TSP	TS	3-DSSP	MMSP
Category	Independent Sales Organization (ISO)	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)	3-D Secure Service Provider (3-DSSP)	Merchant Monitoring Service Provider (MMSP)
Program Service (as defined in the Mastercard Rules manual)	Cardholder and/or merchant solicitation, including application processing Cardholder and/or merchant customer service not affording access to account data, transaction data, or both, including the collection of any fee or other obligation associated with the customer's program Cardholder and/or merchant statement preparation not affording access to account or transaction data Merchant education and training Terminal deployment, not including ATM terminal deployment by an ATM terminal owner that does not perform any other type of ISO Program Service Any other service determined by Mastercard in its sole discretion to be ISO Program Service	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, payment gateway and 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 and/or merchant statement preparation affording access to account data, transaction data, or both Cardholder customer service affording access to account data, transaction data, or both 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 service affording access to account or transaction data and not identified by Mastercard as TPP Program Service or Payment Facilitator Program Service Merchant website hosting or other service involving the computer-based storage of account or 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	Submit to the acquirer records of valid transactions submitted to the Payment Facilitator by a submerchant Timely pay submerchants for transactions submitted to the Payment Facilitator by the submerchant Supply submerchants with all materials necessary to effect transactions through the Payment Facilitator Verify that a submerchant is a bona fide business operation, as set forth in section 7.1.2, “Submerchant Screening Procedures” in Chapter 7 of the Security Rules and Procedures Manual Maintain names, addresses, and URLs if applicable of submerchants Provide recurring education and training to submerchants to ensure compliance with the Standards Monitor the activity and use of the marks of each submerchant for purposes of deterring fraudulent and other wrongful activity	Operates and offers to consumers a Staged Digital Wallet	Account Enablement System Credentials Management System Transaction Management System Trusted Service Manager Any other service specified by Mastercard in its discretion from time to time to be DASP Program Service	Operation of a token vault Token generation and issuance Cardholder authentication and token activation Any other service specified by Mastercard in its discretion from time to time to be TSP Program Service	Any electronically centralized method of administering terminal software service (such as, by way of example and not limitation, service performed by remote access to a terminal) 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	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	Merchant website URL content monitoring Detection of transaction laundering and the monitoring of related activity whereby a merchant or submerchant processes transactions on behalf of another merchant or submerchant with whom the acquirer or the acquirer's Payment Facilitator does not have a merchant agreement or submerchant agreement. Transaction laundering is also referred to as factoring or transaction aggregation.

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]	ISO	TPP	DSE	PF	SDWO	DASP	TSP	TS	3-DSSP	MMSP
		Any other service determined by Mastercard in its sole discretion to be TPP Program Service								
Must be registered by a Mastercard customer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Must validate compliance with the PCI DSS	N/A	Yes	Yes	Yes	Yes	Yes	Yes and PCI TSP Security Requirements	Yes	PCI 3DS Core Security Standard[2]	N/A
SDP Level[3]	N/A	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	N/A
Onsite assessment with a Qualified Security Assessor (QSA) required annually	N/A	Yes	Level 1 DSE: Yes Level 2 DSE: Highly Recommended	Level 1 PF: Yes Level 2 PF: Highly Recommended	Yes	Yes	PCI DSS: QSA PCI TSP Security Requirements: P2PE Assessor	Highly Recommended	PCI 3DS Core Security Standard: 3DS Assessor	N/A
Self-Assessment Questionnaire (SAQ) D-Service Provider required annually	N/A	N/A	Level 2 DSE: Yes	Level 2 PF: Yes	N/A	N/A	N/A	Yes[4]	N/A	N/A
Approved Scanning Vendor (ASV) scans required quarterly	N/A	Yes	Level 1 DSE: Yes Level 2 DSE: Yes	Level 1 PF: Yes Level 2 PF: Yes	Yes	Yes	Yes	Yes - as applicable	Yes	N/A
PCI Attestation of Compliance (AOC) submission to Mastercard annually	N/A	Yes - Send to pcireports@mastercard.com. If a 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.								N/A

[1] Service Provider classifications (for example, TPP, DSE, PF, SDWO, DASP, TSP, TS, or 3-DSSP) 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 Site Data Protection (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 suffered a confirmed Account Data Compromise (ADC) Event will be automatically reclassified to become a SDP Level 1 Service Provider. Compliance validation requirements for Level 1 Service Providers will then apply.

[4] 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 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 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.