

Payment Methods and Validation Requirements

Payment Method	Card-Not-Present, All Cardholder Data Functions Outsourced	Imprint Only, No Electronic Cardholder Data Storage	Standalone, Dial-out Terminal, No Electronic Cardholder Data Storage	Payment Application Systems Connected to the Internet	All Other Methods
<p>Required Characteristics</p> <p><i>A payment method must have all characteristics of one of the first four types to qualify for an abbreviated questionnaire.</i></p>	<ul style="list-style-type: none"> You do not have a face-to-face point-of-sale environment; You handle only card-not-present (e-commerce or mail/telephone-order) transactions; You do not store, process, or transmit any cardholder data on your premises, but rely entirely on a third party to handle these functions; The third party handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant; You retain only paper reports or receipts with cardholder data, and these documents are not received electronically; and You do not store any cardholder data in electronic format. 	<ul style="list-style-type: none"> You use only an imprint machine to take your customers' payment card information; You do not transmit cardholder data over either a phone line or the Internet; You retain only paper copies of receipts; and You do not store cardholder data in electronic format. 	<ul style="list-style-type: none"> You use only standalone, dial-out terminals (connected via a phone line to your processor); The standalone, dial-out terminals are not connected to any other systems within your environment; The standalone, dial-out terminals are not connected to the Internet; You are either a brick-and-mortar (card-present) or e-commerce or mail/telephone order (card-not-present) merchant; You retain only paper reports or paper copies of receipts; and You do not store cardholder data in electronic format. 	<ul style="list-style-type: none"> You have a payment application system (e.g., POS or shopping cart) and an Internet connection on the same device, either because (1) the payment application system is on a personal computer that is connected to the Internet (for example, for email or web browsing), or (2) the payment application system is connected to the Internet to transmit cardholder data; The payment application system/Internet device is not connected to any other systems within your environment; You are either a brick-and-mortar (card-present) or e-commerce or mail/telephone order (card-not-present) merchant; You retain only paper reports or paper copies of receipts; You do not store cardholder data in electronic format; and Your payment application software vendor uses secure techniques to provide remote support to your payment application system. 	<ul style="list-style-type: none"> You do not meet the requirements for any of the other merchant types.
<p>Validation Requirements</p>	<p>Self-Assessment Questionnaire A (13 questions)</p> <p>Possible Onsite Assessment</p>	<p>Self-Assessment Questionnaire B (26 questions)</p> <p>Possible Onsite Assessment</p>	<p>Self-Assessment Questionnaire B (26 questions)</p> <p>Possible Onsite Assessment</p>	<p>Self-Assessment Questionnaire C (41 questions)</p> <p>Possible Onsite Assessment</p> <p>Quarterly Scan</p>	<p>Self-Assessment Questionnaire D (225 questions)*</p> <p>Possible Onsite Assessment</p> <p>Quarterly Scan</p>

Source: Adapted from PCI Security Standards Council, *Payment Card Industry Data Security Standard Self-Assessment Questionnaire—Instructions and Guidelines* (v. 1.2, Oct. 2008).

*While many merchants completing Self-Assessment Questionnaire D will need to validate compliance with every PCI DSS requirement, some merchants with very specific business models may find that some requirements do not apply. The Self-Assessment Questionnaires indicate where the exceptions apply.