

# How do PCI DSS Requirements 2, 6 and 8 apply to SAQ A merchants

PCI SSC FAQ | Article 1439 | May 2019

---

Merchants eligible to complete SAQ A are e-commerce or mail-order/telephone-order (MOTO) merchants that outsource all payment processing and do not store, process or transmit cardholder data on their premises or systems. E-commerce merchants eligible for SAQ A include those that completely outsource all website operations, including those using URL redirect or another mechanism that meets SAQ A criteria to redirect consumers to a compliant third party for payment processing.

Where URL redirection mechanisms to third-party payment processing systems reside on merchant-managed websites, those mechanisms must be protected from ongoing threats, such as man-in-the-middle attacks that aim to manipulate URL redirection mechanisms to direct traffic to malicious sites without the consumers' knowledge. For this reason, requirements for changing default passwords (Requirement 2); implementing basic authentication, such as requiring a unique user ID and strong password (Requirement 8); and installing applicable security patches and ensuring critical patches are applied within one month of release (Requirement 6) are included in SAQ A. These requirements are intended to help protect merchant websites from compromise and maintain the integrity of the redirection mechanism.

In a simple e-commerce environment where the merchant webserver contains the mechanism that redirects customers from their website to a third party for payment processing, the merchant will need to validate these requirements for the webserver upon which the redirection mechanism is located.

It is also possible for a SAQ A merchant to have a more complex e-commerce environment, where additional system components (such as application servers, database servers, and web proxies) control or could impact the integrity of the redirection mechanism. In these scenarios, the requirements would apply to all system components comprising or managing the redirection mechanism.

MOTO or e-commerce merchants that have completely outsourced all operations, including all management of their website, may not have any systems in scope for SAQ A and, in such circumstances, these requirements could be considered "not applicable." If a requirement is deemed not applicable, the merchant should select the "N/A" option for that requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

Source: <https://www.pcisecuritystandards.org/faqs/1439/>