

Why is there a different approach for Direct Post implementations than for iFrame and URL redirect - what are the technical differences and how do they impact the security of e-commerce transactions?

PCI SSC FAQ | Article 1292 | August 2015

The way that criminals attempt to hijack card data from e-commerce transactions depends on the way that the merchant's website accepts cardholder data, the difficulty of gaining access to the transaction, and how likely it is that the criminal will receive an ongoing supply of cardholder data. PCI DSS aims to reduce the probability that a criminal can steal cardholder data from a merchant's e-commerce transaction. In the last three years, the industry has seen two types of attacks against merchant websites which do not directly process cardholder data but which work in conjunction with a payment service provider. Typically these merchants completed SAQ A as they believed that all their payment processing was outsourced. Because of the nature of the attacks, the payment card brands and PCI SSC have clarified the conditions where a merchant can legitimately consider processing to be outsourced.

To be eligible for PCI DSS v3 SAQ-A, the e-commerce environment must be fully outsourced such that: "The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s)." A merchant website can either redirect the consumer to a third-party payment page, or embed the third-party payment page in an iFrame. In either method, the main attack a criminal has against this is to change the code on the merchant's website so the consumer is re-directed to the criminal's payment page and not the legitimate payment page — this is commonly known as a "man-in-the-middle" (MITM) attack. The disadvantage for the criminal is that this attack is usually detected reasonably quickly and minimal cardholder data is put at risk. Additionally some payment service providers are developing solutions that help to detect when a MITM attack has occurred and to notify the merchant accordingly.

Alternatively, there are a number of e-commerce acceptance methods where the merchant website generates the payment page used to collect cardholder data before posting it directly from the consumers' browser to the payment processor. The form elements on this page may be created by HTML loaded from the merchant's website or by JavaScript loaded by the consumer's browser from a third party. From the merchant's perspective this is an attractive solution as it gives the merchant greater control over the look-and-feel of the payment page and the payment flow than what is provided in a redirect or iFrame method. The common criminal attack against this scenario is to compromise the payment page by including criminal-provided JavaScript that simply takes a copy of the cardholder data as it is being entered and sends it to a criminal's server. The actual payment flow is not affected, and therefore this attack is very hard to detect and will often provide an ongoing supply of cardholder data to the criminal. It is primarily for these types of

environments that the Council developed SAQ A-EP to provide a level of assurance that the merchant's website was appropriately protected.

The Council understands that the various ways that merchants can make e-commerce transactions is continually evolving. Merchants and QSAs receive often conflicting advice from vendors which can be especially confusing when the difference between using an iFrame and embedding a payment form in a <DIV> appears to be minimal. However, the difference in security is substantial: fully-hosted payment pages and payment pages loaded into an iFrame are resistant to the transparent theft of cardholder data as it is entered by the consumer; techniques such as Direct Post and JavaScript forms are not. The Council is aware that a MITM attack against a redirect or iFrame is viable, but in the payment brands' experience these are detected before significant volumes of cardholder data are lost. The Council is working with Payment Service Providers to encourage tamper-resistance and tamper-detection which will also reduce the viability of a MITM-type attack.

Where merchants or QSAs are unsure whether the correct SAQ to be completed is SAQ A or SAQ A-EP, they are advised to firstly determine whether "The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s)". If any element of a payment page originates from the merchant's website, the implementation is not eligible for SAQ A. If any element of a payment page originates from a non-compliant service provider, the implementation is not eligible for either SAQ A or SAQ A-EP. If it is unclear whether this condition has been met, merchants or QSAs are advised to contact the acquirer or payment brand.

Source: <https://www.pcisecuritystandards.org/faqs/1292/>