



PCI Compliance for CyberSource

All Harvard Club and SIGs that accept credit cards or debit cards as a form of payment is required by Visa, MasterCard, AMEX and the other card brands to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). CyberSource provides merchant accounts for Harvard Clubs and SIGs and is required to help their merchants achieve PCI DSS compliance. Harvard Clubs and SIGs are also required to provide proof of compliance to CyberSource.

Your transactions are being processed through AlumniMagnet, by CyberSource. AlumniMagnet is PCI compliant and CyberSource has a copy of their PCI compliance certification.

Your Clubs or SIG, as the organization collecting the online payment also needs to verify their PCI compliance. Please see below to determine which SAQ form needs to be filled out and submitted. The majority of Clubs and SIGs only need to fill out the [SAQ A](#) form.

To be eligible to complete SAQ A your Club or SIG must meet ALL of the following conditions:

- Club or SIG does not process any card-present transactions. Meaning that credit card processing happens online and is only user generated.
- Club or SIG does not process credit card payments through the CyberSource virtual terminal or the Authorize.net virtual terminal.
- Club or SIG does not electronically store*, process, or transmit any credit card data on or from any of their locations or facilities but rather outsources all of these functions to PCI compliant third party service providers.
- Club or SIG has confirmed that all third party service providers that handle credit card data on their behalf are PCI compliant.

** Storage of paper reports and paper receipts containing credit card data is permitted as long as the reports and receipts are NOT received electronically such as via email.*

Some Clubs and SIGs have decided to use another third party company to submit the PCI compliance documents. This is an OPTIONAL service that includes a fee. Trustwave Trustkeeper is a verified partner as part of the CyberSource PCI Compliance Program.

IMPORTANT: If your Club or SIG decides to use Trustwave – you will need to contact your TrustWave rep and change your domain's status. The nature of your website is such that payments are not collected directly on your domain. Your website is hosted by OmniMagnet which collects the payments on your behalf by redirecting customers to their site. This means that you do not require monthly vulnerability scans and, in some cases, your Self-Assessment Questionnaire (SAQ) may be shorter. You should call Trustwave at (800) 213-8918 in order to verify that your merchant categorization is correct and, if not, Trustwave will consult with your credit card processor for approval. Please be sure to mention that your website redirects customers to a third party in order to process payments. Trustwave can assist you with removing scan targets if scanning is no longer required.