VISION™

Online Payments & PCI Compliance

For online payments with both PayPal and Authorize.NET, we don't store any credit card information in our website for the online payments component. We also force our clients to enable SSL in all payment pages. As a result, our website follows PCI compliance.

For Online Payments, we handle transactions in the following way:

PayPal:

We use PayPal Payments Standard integration. This uses a HTML form to redirect to PayPal, then users input their credit card or login with a PayPal account to conduct the transaction.

Authorize.NET:

We use DPM (Direct Post Method) integration. Here, users input credit card information on our website, but we post all this information into Authorize.NET, and we don't store any credit card information. More details on the DPM:https://community.developer.authorize.net/t5/The-Authorize-Net-Developer-Blog/Direct-Post-Method-DPM/ba-p/7014

We may also add some language to contracts to guide our clients so that they do not store documents/images with credit card data, and so that they are aware that they should not use the forms and surveys component, the RAD editor, or other components not designated for online payments to request such information. So, it is also partly their responsibility to ensure that they are not requesting credit card information in other areas of the website.

Please see below for additional
information on Authorize.NET and Heartland.

Authorize.NET: http://www.authorize.net/solutions/merchantsolutions/merchantservices/security/

Heartland:
http://www.heartlandpaymentsystems.com/payment-processing/