

Streamline Sales Using Silent Order Post (SOP)

CyberSource Payment Security



Providing your customers with a seamless ecommerce checkout experience is critical to a merchant's brand image. As attention spans shorten and intolerance of purchase process hiccups increases, merchants must strive to provide the quickest decision-to-buy flow possible. In addition, adhering to PCI DSS standards on how credit card information is processed, transmitted, and stored can get costly. This brief will discuss the use of a Silent Order Post (SOP) to provide customers with the checkout experience they require while achieving continuous PCI compliance.

What is a Silent Order Post (SOP)?

The Silent Order Post is the back-end technology behind the "buy" button on your website that routes payment data to a third-party, PCI-compliant vendor (such as CyberSource) for processing. To the customer making a purchase on your website, it is entirely seamless as your branding remains consistent throughout. The entire process of entering in personal payment data is transparent as no re-directs to CyberSource are required.

To use this solution, you store an HTML order form on you web server. When the customer is ready to checkout, they would enter their payment data into the fields including name, shipping address, account number, etc. The payment fields are hosted by CyberSource, thereby bypassing your environment entirely. The captured payment data is transmitted directly from the customer's browser to CyberSource for processing, storage of the credit card data, and tokenization of the PAN.

You receive a reply back from CyberSource as to whether or the transaction was successful or failed along with the tokenization related to that transaction. Based on that reply, you can direct the customer to the appropriate results page including a 'thank you' for successful transactions or 'try transaction again' for a failure. You then ship the order. Reference the graphical representation available on Page 2.

PCI Compliance using the SOP

Merchant who process, transmit, or store credit card information are within scope of the PCI requirement. PCI defines these behaviors as follows:

- Processing – refers to the act of storing and/or manipulating a credit card account number in a computer system's memory.
- Transmitting – is the act of sending a credit card account number from one computer system to another.
- Storing – is the act of retaining credit card numbers, CVN, or CVV2 data on a hard drive or other permanent digital storage medium.

Why choose Silent Order Post?

- Maintains consistent corporate branding
- Fully customizable user interface
- Enables tracking of shopping cart statistics through to purchase and authorization results
- Removes credit card information entirely from the environment
- Significantly reduces scope of PCI-DSS
- Supports international language support
- Multiple payment options are available: credit cards, e-checks, tokenization, etc.
- Integrates seamlessly with complimentary CyberSource Fraud services

CyberSource®
the power of payment

Streamline Sales Using Silent Order Post (SOP)



Page 2

In using the SOP plus tokenization processing, transmitting, and storing of credit card data never occurs in your environment. CyberSource would also provide the Secure Sockets Layer (SSL) Certificate, as the customers' sensitive information would be encrypted during transmission within CyberSource's environment.

Use of the SOP does not, however, negate the need to validate PCI compliance. However, because many of the controls will be considered "not applicable," Level 2, 3, and 4 merchants will only need to complete a PCI-DSS Self-Assessment Questionnaire (SAQ) A, which contains thirteen 'yes' and 'no' answers. In comparison, an average large merchant would be required to submit a fifty-page in-depth questionnaire as well as evidence of passing vulnerability scans completed by a PCI SSC Approved Scanning Vendor (ASV), a process that could take months to complete. Level 1 merchants will still be required to be audited by an authorized QSA, but the scope of that audit will be dramatically reduced.

Handling future transactions with tokenization

The token that is returned to you following the customer's initial purchase can be stored in your ERP or other system of record for future transactions. These types of transactions include additional purchases, authorizations, credits, chargebacks, recurring billing, split shipments, settlement, and reconciliation. You need only provide CyberSource with the intended transaction amount and the associated customer token to facilitate the request.

Additional benefits of the SOP

Customization – The SOP provides you with the ability to create a seamless checkout environment for you customers. The payment page retains the same branding as the rest of the site and the page URL does not change as re-directs are not required*.

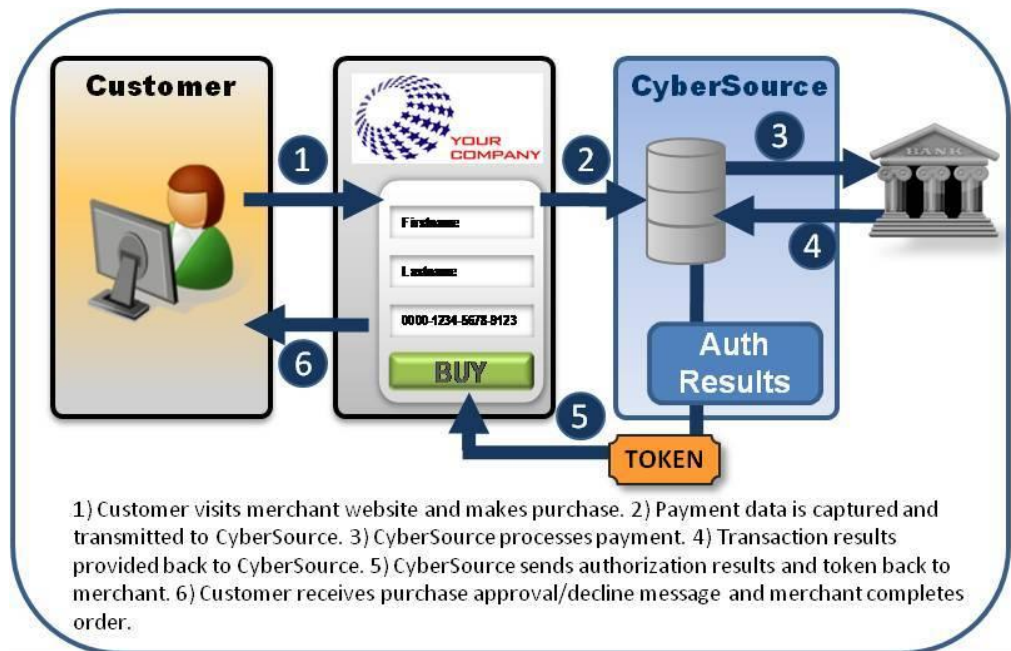
Simplicity – The implementation of the SOP is simple. A client application is not required as you can simply use Simple Order API fields.

Processing capabilities – The SOP can process e-checks as well as credit cards.

CyberSource Integration – The SOP integrates seamlessly with the CyberSource Decision Manager to accurately identify and review potentially risky transactions while minimizing the rejection of valid order.

Analysis – You can track customer statistics and behavior using shopping cart analysis as the SOP provides an end-to-end buying experience.

*The Hosted Order Page (HOP) is entirely hosted by CyberSource, so a re-direct is necessary. Branding is retained as the page is customizable.



CyberSource[®]
the power of payment