



ELEMENT PAYMENT SERVICES, INC.

HOSTED PAYMENTS

REMOVING SOFTWARE VENDORS
FROM THE SCOPE OF PA DSS

*Written by Don Schroeder
Chief Technology Officer, Element Payment Services, Inc.*

WHITE PAPER

Confidential & Proprietary

1	INTRODUCTION.....	4
2	PURPOSE.....	5
3	COMPANY BACKGROUND	6
4	PROBLEM.....	8
4.1	VISA SECURITY MANDATES	9
4.2	PA DSS SCOPE	10
4.3	PA DSS COMPLIANCE.....	11
4.3.1	<i>Report Acceptance Process</i>	<i>13</i>
4.3.2	<i>Change to Application Process</i>	<i>14</i>
4.3.3	<i>Annual Revalidation and Renewing Expired Applications Process.....</i>	<i>15</i>
5	SOLUTION	16
5.1	HOSTED PAYMENTS	16
5.2	HOSTED PAYMENT WINDOW.....	17
5.3	HOSTED PAYMENT PAGE.....	19
6	SUMMARY	21

NOTE: By its acceptance and review hereof, the recipient agrees that neither it nor its agents, representatives, directors or employees will copy, reproduce or distribute to others this White Paper, either in whole or in part, at any time without the prior written consent of Element Payment Systems, Inc. and will keep permanently confidential all information contained herein which is not already in the public domain.

1 Introduction

To appreciate the benefits of Element's new Hosted Payments, it's important to first understand the origins of the Payment Application Data Security Standards ("PA DSS"), and to understand how the PA DSS relates to, and is dependent on, the Payment Card Industry Data Security Standards ("PCI DSS").

The requirements for PA DSS are based on, and derived from, PCI DSS. PCI DSS is a comprehensive set of requirements that applies directly to merchants and payments service providers. PCI DSS describes in great detail all of the necessary requirements to ensure a secure environment for accepting cardholder data. This includes any software applications within the environment that store, process, or transmit cardholder data. PCI DSS, however, does not directly apply to the merchants' software vendors. Because the software vendors do not store, process, or transmit cardholder data they are not directly in scope of PCI DSS. Software vendors' applications, however, should facilitate and not prevent their customers/merchants from complying with PCI DSS. This is the origin and catalyst for PA DSS.

PA DSS applies directly to any software vendor's application sold, distributed, or licensed to third parties that stores, processes, or transmits cardholder data.

The benefit of Element's Hosted Payments is that it provides software vendors with the ability to deliver fully integrated payment solutions without the need to store, process, or transmit cardholder data; thus removing them from the scope and difficulty of PA DSS compliance.

2 Purpose

The purpose of this document is to describe how Element Payment Services, Inc's. new Hosted Payments services can remove software vendors from the scope of the PA DSS; and eliminate the untold time and expense which will be required to achieve and maintain PA DSS compliance. With Hosted Payments software vendors can also remove a significant financial risk related to providing applications that include integrated payment solutions. The expected audience is software vendors and others who develop applications that store, process, or transmit cardholder data.

3 Company Background

About Element Payment Services, Inc. (www.elementps.com)

Headquartered in Phoenix, Arizona, and founded by payment industry experts, Element Payment Services Inc. provides secure, reliable and innovative payment processing solutions directly to merchants through partnership with leading business management software providers.

Processing an estimated \$4 billion in annual transaction volume for 30,000 merchants, Element's PCI DSS compliant Express Processing Platform supports credit, debit, check conversion and guarantee, and ACH processing solutions.

Because the company develops and supports all of its technology in-house, Element is able to offer unparalleled security, ease-of-use and customer service for both merchants and software providers.

Easy to Integrate for Software Providers and Merchants– Business management software is easy to integrate to the Element Express Processing platform through the support for XML and Web services interfaces and service-oriented architecture.

A Fully Integrated Solution - Once business management software is integrated with Element Express, merchants can manage their entire business, and securely process payments within the same application.

Easily Comply with PCI DSS Requirements – The Element Express Processing Platform allows software providers and merchants to easily comply with industry compliance requirements such as PCI DSS, PA DSS (PABP).

Superior Customer Service – Element offers 24 x 7 support services from technically trained customer care specialist via toll-free telephone and e-mail.

About Our Software Partners

Element partners with leading business management software providers to offer their customers a fully-integrated, PCI DSS compliant payment processing solution.

Element's partners specialize in business management software for all industry types including spa/salon, pest control, veterinary, healthcare/medical, industrial, educational/performance arts and facilities management.

About Our Merchants

Element provides payment processing services to merchants of all types throughout the United States.

For more information about Element Payment Services, please visit www.elementps.com or contact us at **1.866.435.3636**

Element Payment Services Inc. is a registered Merchant Service Provider with First National Bank of Omaha.

4 Problem

Several years ago, Visa developed the Payment Application Best Practices (“PABP”). The purpose of the program was to assist software vendors in creating secure payment applications to help merchants mitigate cardholder compromises and prevent storage of sensitive cardholder data (i.e. full magnetic stripe data, CVV, CVV2, or PIN data). Essentially, the goal is to support overall compliance with the PCI Data Security Standard.

Since inception, however, PABP has had only limited success in its endeavor as there has been no widespread adoption of the so called “Best Practice”. Without mandates or penalties, software vendors lacked a viable business case to justify the inordinate time and expense required to achieve compliance with PABP. All that changed on April 15, 2008.

Due to the steady increase in the frequency of cardholder data compromises, the PCI Security Standards Council (“PCI SSC”) published version 1.1 of the PA DSS. In doing so, the PCI SSC effectively transitioned Visa’s PABP into an enforceable security standard. In addition, Visa has also outlined strict set mandates (see Visa Security Mandates below) including very aggressive compliance dates required for implementing PA DSS.

Now that the PABP has been transitioned to PA DSS and Visa has mandated aggressive timelines enforcing compliance; software vendors in scope of PA DSS must devote an inordinate amount of time and expense to achieving and maintaining compliance with PA DSS.

4.1 Visa Security Mandates

On January 1, 2008 Visa issued a series of strict mandates in an effort to eliminate the use of vulnerable payment applications from the Visa payment networks. Visa states: “These mandates require acquirers to ensure that their merchants and agents do not use payment applications known to retain sensitive cardholder data elements (i.e. full magnetic stripe data, CVV, CVV2 or PIN data) and require the use of payment applications that adhere to the PA DSS.”

Below are the five mandates that take effect over the next three years:

Phase	Compliance Mandate	Effective Date
I	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	1/1/08
II	VNPs and agents must only certify new payment applications to their platforms that are PA DSS-compliant	7/1/08
III	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PA DSS-compliant applications*	10/1/08
IV	VNPs and agents must decertify all vulnerable payment applications**	10/1/09
V	Acquirers must ensure their merchants, VNPs and agents use only PA DSS-compliant applications***	7/1/10

* In-house use only developed applications & stand-alone POS hardware terminals are not applicable

** VisaNet Processors (VNPs) and agents must decertify vulnerable payment applications within 12 months of identification

*** Date is aligned with TDES mandate for all POS PEDs to support TDES and be Visa-Approved/Lab-Evaluated

Two key dates outlined above for software vendors are 7/1/08 and 10/1/08.

As of July 1, 2008, payment processors (i.e. VNPs) cannot certify software applications that are not PA DSS validated. The purpose of this mandate is to prevent any further proliferation of non-PA DSS software. This means that if a software vendor’s application is not PA DSS compliant they cannot certify their solution with any payment processors.

Beginning October 1, 2008, all Level 3 and 4 merchants (see Merchant Level Description below) must be PCI DSS compliant and/or use PA DSS compliant applications. The purpose of this mandate is to prevent any Level 3 and 4 merchants from using any non-PA DSS compliant software application. If a software vendor’s application is not PA DSS compliant after this date, Level 3 and 4 merchants cannot use their software to process, store, or transmit cardholder data.

Merchant Level*	Description
1	Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 Visa transactions per year.
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year.

4.2 PA DSS Scope

According to the PCI Security Standards Council, “the PA DSS [scope] applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.” Additionally, “PA DSS does apply to payment applications provided in modules, which typically includes a ‘baseline’ module and other modules specific to customer types or functions ... If other modules also perform payment functions; PA DSS applies to those modules as well.” Therefore, the scope of PA DSS, as defined by the PCI Security Standards Council, includes not only stand alone payment applications; but also applications that integrate to payment applications if they perform payment functions.

Note:

Software vendors that integrate to payment applications are in scope of PA DSS according to the PCI SCC because they are directly involved in the collection, input, and transmitting of cardholder data; and because their software contains modules that perform payment functions.

4.3 PA DSS Compliance

Software vendor applications that are in scope must comply with PA DSS. PA DSS compliance requires the concerted efforts of the following three parties; 1) software vendors, 2) Payment Application Qualified Security Assessors (“PA QSA”), and 3) the PCI SSC. Each of these parties has its own distinct set of responsibilities.

Software Vendors are responsible for the following:

- Creating PA DSS compliant payment applications that facilitate and do not prevent their customers’ PCI DSS compliance (The application cannot require an implementation or configuration setting that violates a PCI DSS requirement.)
- Following PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting)
- Creating a *PA DSS Implementation Guide*, specific to each application, according to the requirements in the *Payment Application Data Security Standard*
- Educating customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS compliant manner
- Ensuring payment applications meet PA DSS requirements by successfully passing a PA DSS review

PA QSAs are responsible for:

- Performing assessments on payment applications in accordance with the Security Audit Procedures and the PA QSA Validation Requirements
- Providing an opinion regarding whether the payment application meets PA DSS requirements
- Providing adequate documentation within the Report of Validation (ROV) to demonstrate the payment application’s compliance with the PA DSS
- Submitting the ROV to PCI SSC, along with the Attestation of Validation (signed by both PA QSA and vendor)
- Maintaining an internal quality assurance process for their PA QSA efforts

PCI SSC:

- Is a centralized repository for PA DSS ROVs
- Performs Quality Assurance reviews of PA DSS ROVs to confirm report consistency and quality
- Lists PA DSS validated payment applications on the PCI SSC Web site. *Note: this list will not be available on the Web site until after September 30, 2008*
- Qualifies and trains PA QSAs to perform PA DSS reviews
- Maintains and updates the PA DSS standard and related documentation according to a standards lifecycle management process

To ensure that software vendors meet the PA DSS requirements, they must successfully pass a PA DSS review. PA DSS reviews are performed by independent assessors known as PA QSAs. It is the responsibility of the software vendor to locate and pay for a PA QSA to perform their review.

The goal of a PA DSS review is to produce a ROV. The ROV is subsequently submitted to the PCI SSC for approval and listing on the PCI SSC Web site. In addition to the PA QSA fees, the software vendor is also responsible for paying the PCI SSC a quarterly listing fee. This fee is for listing the software vendor's application on the PCI SSC Web site.

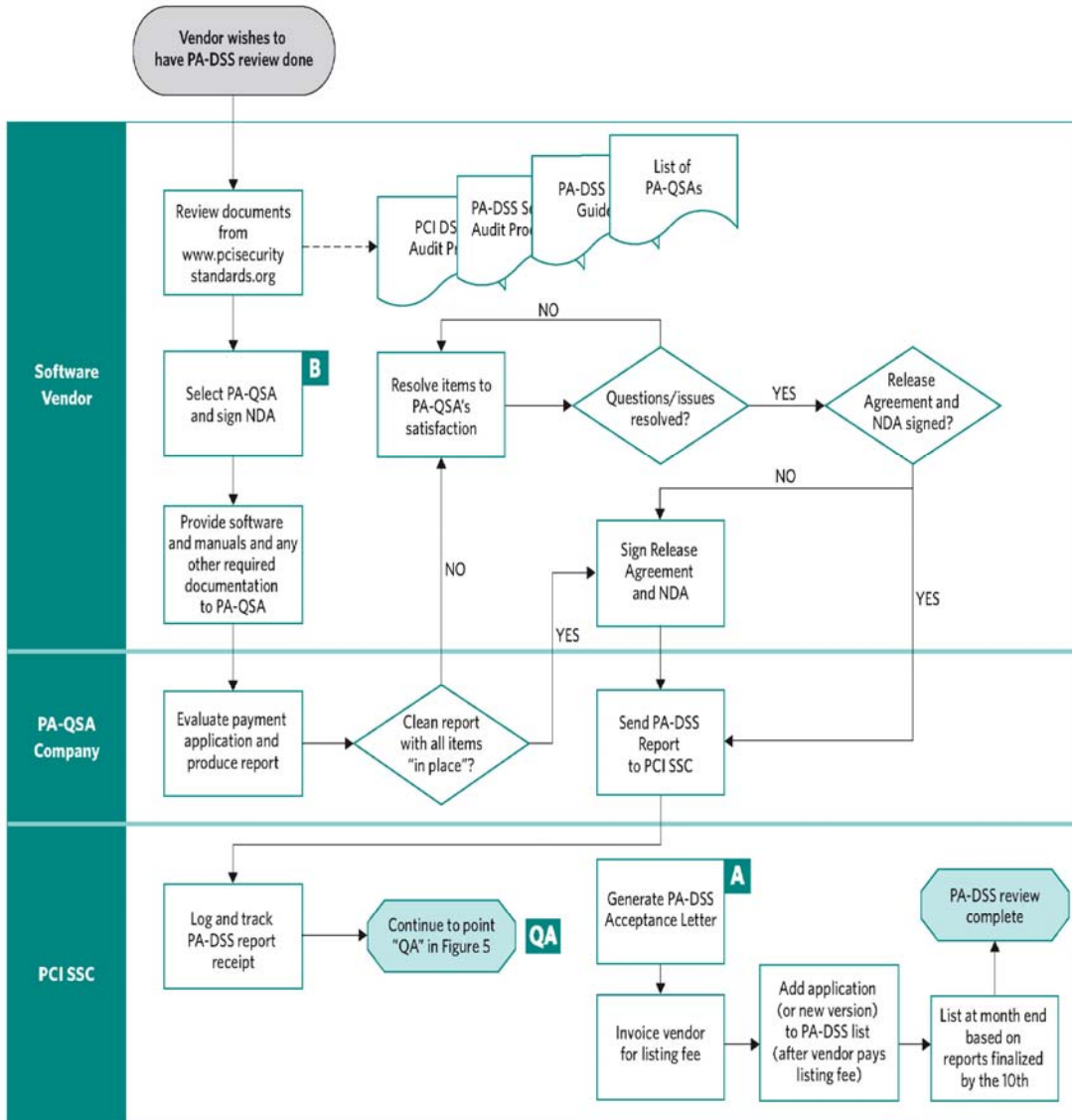
Note:

There are significant costs related to achieving and maintaining PA DSS compliance. These costs are the sole responsibility of the software vendor.

The following three flow diagrams depict the entire complex lifecycle of the PA DSS review process:

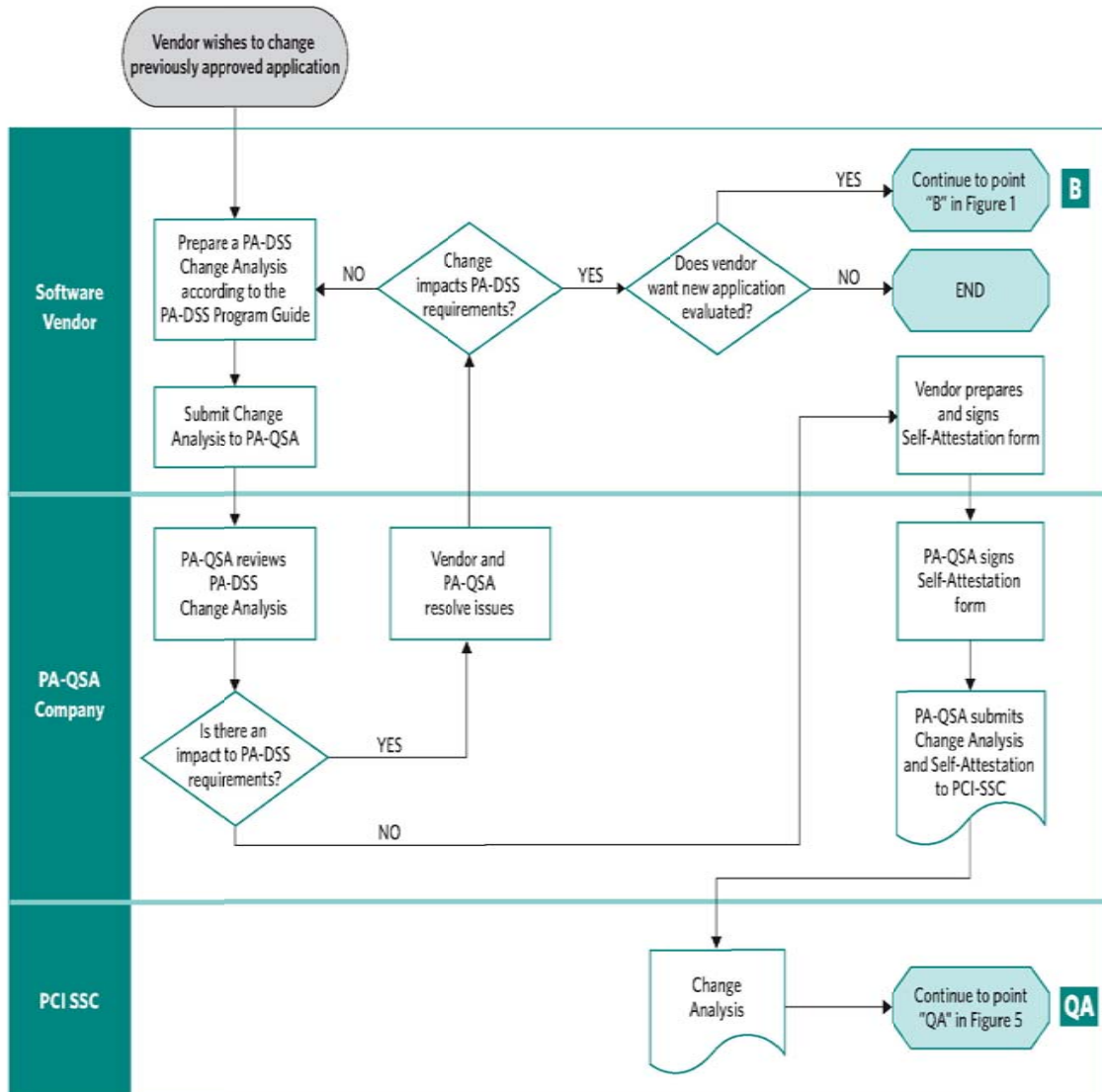
4.3.1 Report Acceptance Process

The Report Acceptance Process is the first step that software vendors must take to become PA DSS.



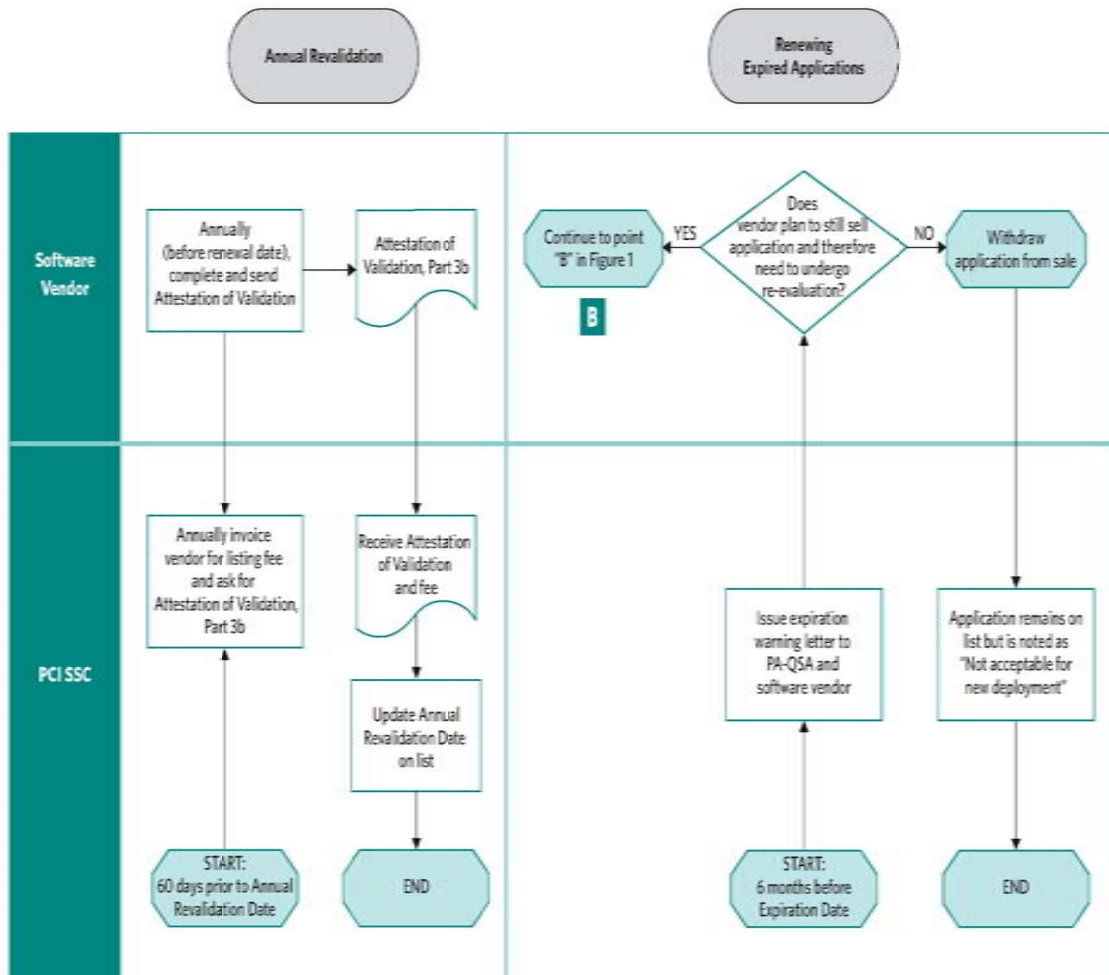
4.3.2 Change to Application Process

The Change to Application Process is what a software vendor must do every time a change is made to their software.



4.3.3 Annual Revalidation and Renewing Expired Applications Process

The Annual Revalidation and Renewing Expired Applications Process is what the software vendor must do every year to maintain their PA DSS compliance.



5 Solution

Element has developed a new technology called Hosted Payments which is specifically designed to remove software vendors from the scope of PA DSS. By being removed from scope software vendors can eliminate time and expense related to achieving and maintaining compliance with PA DSS. In addition, software vendors can also remove a significant financial risk related to providing their customers with fully integrated payment solutions.

5.1 Hosted Payments

According to the PCI SSC, the scope of PA DSS applies to software vendors that store, process, or transmit cardholder data. If software vendors do not store, process, or transmit cardholder data, by definition they are not in scope. By shifting the responsibility of handling the cardholder data, Hosted Payments eliminates the need for software vendors to be PA DSS compliant.

How does it work? Element offers two types of Hosted Payments: 1) Hosted Payment Windows for distributed software applications (see section 5.2 below); and 2) Hosted Payment Pages for Web based software applications (see section 5.3 below).

Both types of Hosted Payments essentially work in the same way. The software vendor's application is responsible for collecting all of the non-sensitive data needed to perform a payment transaction; while Element's Hosted Payments is responsible for collecting, storing, processing and transmitting all the sensitive cardholder data. In addition, by taking advantage of Element's extensive real-time reporting application presentation interface ("API") capabilities software vendors can enjoy all of the benefits inherent to fully integrated payment solutions without the risks associated with handling cardholder data.

5.2 Hosted Payment Window

Below is a step-by-step demonstration of how a Hosted Payment Window can seamlessly integrate with a typical point of sale (“POS”) software application:

1. POS software application collects all of the non-sensitive data related to a purchase.

Item Lookup Code	Description	Quantity	Price
11300	Baseball	1	\$10.99
11312	Bat	1	\$179.99
11315	Hat	1	\$24.82
11399	Shirt	1	\$24.99

Sub Total	Sales Tax	Total
\$240.79	\$24.08	\$264.87

2. POS software application calls the Hosted Payment TransactionSetup method to obtain a TransactionSetupID that will be used from this point forward to uniquely identify this purchase.
3. POS software application displays a window or form containing an embedded Web browser control and navigates the control to Element’s Hosted Payments: [https://www.hostedpayments.com/?TransactionSetupID=\[Insert TransactionSetupID here\]](https://www.hostedpayments.com/?TransactionSetupID=[Insert TransactionSetupID here]).

Cardholder Data

Credit Card Information * Denotes a required field

*Card Number:

*Expiration: Month / Year

CVV:

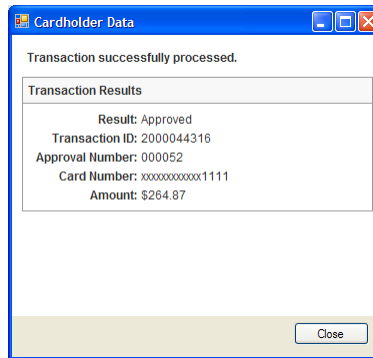
Transaction Information

Amount: \$264.87

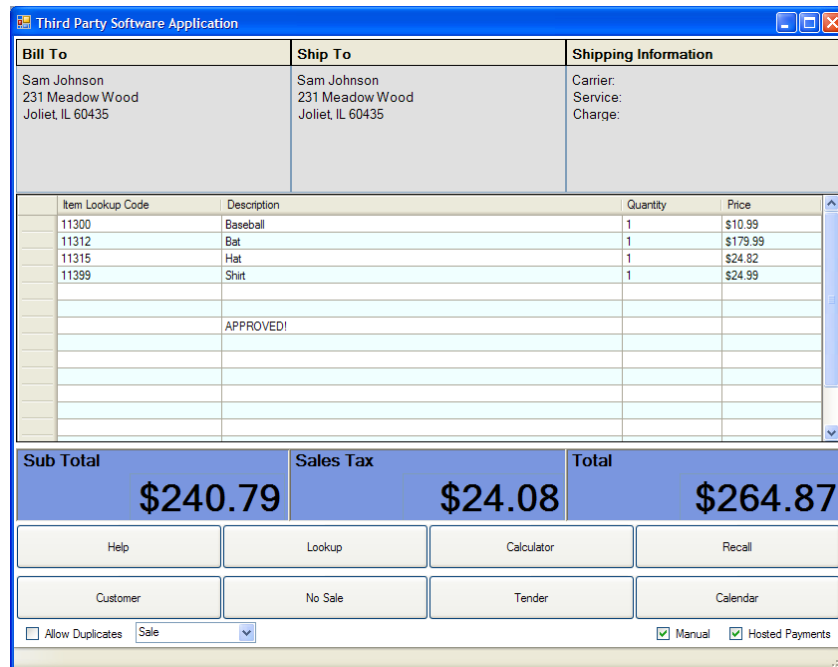
PROCESS TRANSACTION > [Cancel Transaction](#)

Close

- Element's Hosted Payment Window collects, stores (if applicable), processes, and transmits all the sensitive cardholder data; and displays the result of the transaction. In addition, the result of the transaction is embedded in the response window to provide a synchronous way for the application to know the status of the transaction.



- In addition to knowing the status of the transaction through the method described above; the POS software application can also programmatically query Element's real-time reporting API, using the TransactionSetupID for this purchase, to asynchronously obtain the status of the transaction.



5.3 Hosted Payment Page

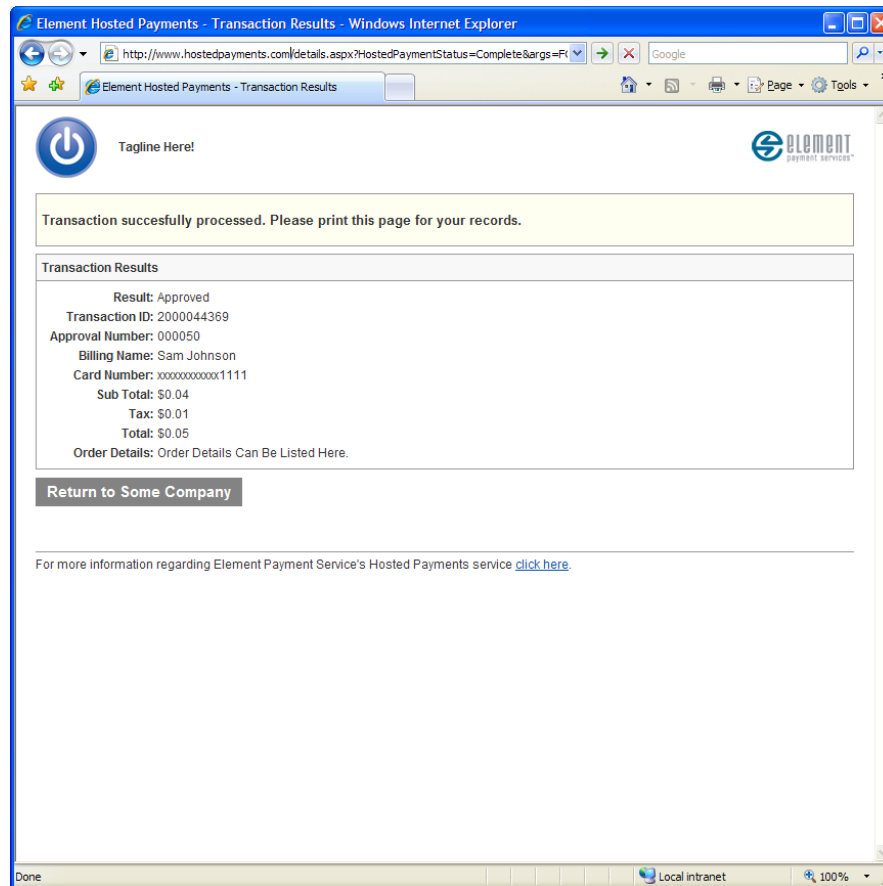
Below is a step-by-step demonstration of how a Hosted Payment Page can seamlessly integrate with a typical web based software application:

1. Web based software application collects all of the non-sensitive data related to the purchase.
2. Web based software application calls the Hosted Payment TransactionSetup method to obtain a TransactionSetupID that will be used from this point forward to uniquely identify this purchase.
3. Web based software application redirects form their site to Element's Hosted Payments: [https://www.hostedpayments.com/?TransactionSetupID=\[Insert ID here\]](https://www.hostedpayments.com/?TransactionSetupID=[Insert ID here]).

The screenshot shows a web browser window titled "Element Hosted Payments - Process Transaction - Windows Internet Explorer". The address bar shows the URL: <https://www.hostedpayments.com/?TransactionSetupID=2CBA134B-56FB-4536-A3F1-961>. The page content includes:

- A power button icon and the text "Tagline Here!".
- The Element Payment Services logo.
- A yellow box with the text: "To complete your secure transaction from Some Company enter credit card information below and click process transaction." Below this is a link: "Learn why it's safe to pay with [Element Hosted Payments](#)."
- A section titled "Credit Card Information" with a red asterisk and the text "* Denotes a required field". It contains three input fields: "*Card Number:", "*Expiration: Month / Year", and "*CVV:".
- A section titled "Transaction Information" with the following details:
 - Reference #: 11399383334
 - Sub Total: \$0.04
 - Tax: \$0.01
 - Total: \$0.05
- A section titled "Order Details" with the text "Order Details Can Be Listed Here."
- A section titled "Address Information" with two columns: "Billing Address:" and "Shipping Address:". Both columns list the same address: Sam Johnson, 222 West State Apt. 4, Phoenix, AZ 85014, 602-334-3557, sam@email.com.
- At the bottom of the form, there are two buttons: "PROCESS TRANSACTION >" and "Cancel and return to Some Company".
- At the very bottom, there is a link: "For more information regarding Element Payment Service's Hosted Payments service [click here](#)."

4. Element's Hosted Payment Window collects, stores (if applicable), processes, and transmits all the sensitive cardholder data; and displays the result of the transaction. In addition, the result of the transaction is embedded in the redirect URL to provide a synchronous way for the Web based software application to know the status of the transaction.



5. In addition to knowing the status of the transaction through the synchronous method mentioned above; the Web based software application can also programmatically query Element's real-time reporting API, using the TransactionSetupID for this purchase, to asynchronously obtain the status of the transaction.

6 Summary

Given the steady increase in cardholder data compromises and the ensuing security mandates, software vendors have no choice other than to comply with PA DSS.

The critical choice they face is to either take on the expensive burden of achieving PA DSS compliance independently or implement Element's new Hosted Payments solution.

By integrating with the Element Express Processing Platform, software providers not only avoid these hassles and cost of achieving compliance but are also able to offer their customers the highest level of protection from cardholder data compromises. Because the Express Processing Platform meets PCI DSS compliance requirements which exceed the security mandates of PA DSS merchants are better protected completing a Hosted Payment integration and creating an even greater competitive differentiator for software providers.