element payment services™

Interface to Security

Element Payment Services

Payment Card Industry Compliance FAQ for Independent Software Vendors (ISVs)

PA-DSS and PCI DSS Compliance can be confusing—especially for Software Providers. Our Payment Card Industry Compliance FAQ for Independent Software Vendors (ISVs) is designed to arm you with the facts and help you get started on the road to compliance.

Does Your Application Transmit Cardholder Data?

If in your application, cardholder data is directly entered (this could be as simple as a text box input) then the answer is yes.

Unfortunately, answering yes to this question also means your software application is considered a payment application by the Payment Card Industry Security Standards Council (PCI SSC) and, therefore, is in scope of the Payment Application Data Security Standard (PA-DSS).

PA-DSS SCOPE DEFINED

The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization and settlement, where these payment applications are sold, distributed, or licensed to third parties.

Compliance Concerns
for Software Providers

Q: What is PA-DSS (PABP) Compliance?

A: Several years ago, Visa developed the Payment Application Best Practices (PABP). The purpose of the program was to guide software vendors in creating secure applications, as well as support merchant compliance with the Payment Card Industry Data Security Standard (PCI DSS). Since its inception, however, there has been no widespread adoption of PABP. 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, when the PCI Security Standards Council published the Payment Application Data Security Standard (PA-DSS). In doing so, Visa's PABP was effectively transitioned into an enforceable security standard.

Software applications must now successfully pass a PA-DSS review—performed by PA QSAs—or go out-of-scope of compliance requirements. The Payment Card Industry Security Standards Council lists PA-DSS compliant applications on their web site at **www.pcisecuritystandards.org.** Not being on that list, or out-of-scope of PA-DSS, could mean damage to a software provider's brand, financial liability or, perhaps worse, a loss of sales to merchants for whom PCI DSS compliance is essential.

Q: How Can I Make Sure My Software is Compliant?

A: Element offers two innovative solutions to help software providers become PA-DSS compliant. One is direct integration with Element's payment processing system, Element Express. The other is called Hosted Payments, which fully removes your application from the scope of PA-DSS compliance, along with the burden and risk.

DIRECT INTEGRATION

When your software is integrated with the Element Express platform, merchants get the benefits of reduced risk, optimal security and compliance with PCI DSS. That means less risk for you, easier compliance with PA-DSS (PABP) and, most importantly, merchants who are more satisfied with your software solution. Today, many vendors offer semi-integrated and multi-integrated systems that require the maintenance of distributed software or introduce multiple points of failure—and cost—into the payment process. **Element's directly integrated solution helps strengthen your brand and your revenue by providing your merchants assured security coupled with the best possible service and support.**

By integrating your software with Express, you get:

- Fewer security worries because Element provides built-in compliance with current and future PCI DSS security requirements.
- Less hassle and cost because there's no need to update your application to accommodate new versions of distributed, third-party payment software.
- More satisfied merchants who are getting higher quality processing services and better support because there's only one player—Element—in the payment stream.
- Higher customer retention because with the Express platform working for your merchants, there's less reason for them to switch software providers.

HOSTED PAYMENTS

Element's Hosted Payments allows software providers to remain out of scope for PA-DSS (PABP), and avoid the significant cost and effort of achieving validation. With Hosted Payments, your application is responsible for collecting all of the non-sensitive data needed to perform a payment transaction. Element then handles all of the sensitive cardholder data—leaving your application free of information susceptible to data thieves.

By shifting the responsibility of storing, processing, and transmitting sensitive cardholder data to Element, Hosted Payments removes your software application from the scope of PA-DSS (PABP) compliance. Software vendors not only avoid the hassle and cost of achieving compliance, but because Hosted Payments is integrated with the PCI compliant Express platform, you are able to offer your customers the highest level of protection from cardholder data compromises. In addition, with Element's real-time reporting capabilities, you and your customers enjoy all of the benefits of a fully integrated payment solution.

Element offers Hosted Payments for both distributed and Web-based software applications. Both solutions seamlessly integrate with all types of business management software applications.

Element's Hosted Payments enables you to:

- Eliminate the need for PA-DSS (PABP) compliance
- Reduce risk associated with storing sensitive cardholder data
- Leverage our PCI DSS compliant platform
- Provide your customers the highest level of data protection
- Benefit from real-time reporting

Q: Why Should I Be Compliant?

A: All software providers must meet PA-DSS requirements for their customers to comply with the mandated Payment Card Industry Data Security Standard (PCI DSS). As of October 1, 2008, acquiring financial institutions cannot approve merchants for processing that are using non-compliant software. *Software providers with applications that don't meet PA-DSS (PABP) compliance requirements are beginning to lose customers and revenue as a result.*

Q: What are the Costs of Direct Integration Relative to PA-DSS Compliance?

A: While Element does not charge a fee for integrating to Express, software providers who elect to directly integrate their applications remain in-scope for PA-DSS and are required to undergo validation. This involves a security audit from a PA-DSS (PABP) Qualified Security Assessor (QSA) and the development time and expense to bring their application into compliance. These costs can range from tens to hundreds of thousands of dollars. Additionally, software providers are required to pay $1,250 annually per software application to have their solutions lists as a validated PA-DSS-compliant solution: **www.pcisecuritystandards.org/security_standards/vpa.**

Q: What is the Cost of Hosted Payments?

A: Element does not charge for Hosted Payments. As software providers are exempt from PA-DSS validation when they use Hosted Payments, the only cost incurred is the development time to integrate to Hosted Payments, which for most partners takes less than a week.

COST COMPARISON:
PA-DSS (PABP) Certification vs. Element's Hosted Payments

	Element Payment Services	Payment Card Industry Security Standard Council (PCI-SCC)
	Hosted Payments	PA-DSS Validation
Timeline	1-2 Weeks	3-9 Months
Annual Listing Fee	N/A	$1,250
PA-DSS Validation Expense	N/A	$20,000 – $30,000
Development Expense to Achieve Validation*	N/A	$15,000 – $30,000
Initial Fee	No Fee	$36,250 – $61,250
Annual Maintenance Expense**	No Fee	$20,000 – $30,000

*Application developers are generally required to make changes to their application following the security assessment. Estimate is based on development expense to bring the application into compliance.

**Costs associated with annual revalidation requirements.

Q: What is PCI DSS Compliance and How Does it Relate to the PA-DSS?

A: Payment Card Industry Data Security Standard (PCI DSS) requirements were created by the major credit card companies to protect cardholder data from a rising tide of hackers and thieves. Compromised credit card and personal information has cost major retailers hundreds of millions of dollars in fines and compensation to customers. There are also less obvious costs resulting from data breaches, such as lost sales or damage to merchants' brands. PCI DSS compliance is not an option but a *requirement* for any merchant, bank or processor who handles payment card information. **Software developers and integrators that store, process or transmit such information are also required to be PCI compliant, according to the Payment Application Data Security Standard (PA-DSS).**

Element Payment Services helps you become PA-DSS compliant with advanced security features that simplify the validation process. We also help your customers comply with PCI DSS by enabling end-to-end credit card encryption and off-site storage of sensitive data. Our in-depth expertise—enhanced by membership on the Payment Card Industry Security Standards Council—will help you not only comply with but understand PCI DSS. We give your merchants the fastest, most cost-effective payment processing on the market.

At Element, We're Here to Help

If you're feeling overwhelmed by the cost and complexity of achieving PA-DSS Compliance, we understand. You built your business by understanding the needs of merchants and creating business software to meet those needs, not by being expert in data encryption or the definition of "sensitive cardholder data."

Your expertise is serving your customers. Our expertise is compliant payment processing. Let us help. Contact us with your compliance questions today at **1.866.435.3636 x764** or **www.elementps.com**.