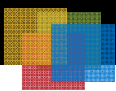


# Payment Application Security

*The Payment Application Data Security Standard (PA-DSS) builds upon and expands established best practices to ensure that payment applications do not store sensitive card data. This mandated standard has requirements and ramifications for all participants in the payment industry.*



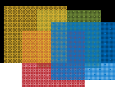
## Executive Summary

Security of payment card transactions is a paramount issue to merchant and acquirer alike, whether through a desire to protect their customers, or simply the need to comply with industry-wide requirements.

Payment Application Data Security Standard, or PA-DSS, is the latest component of Payment Card Industry (PCI) standardized requirements established by the PCI Security Standards Council (PCI SSC).

PA-DSS builds upon and expands best practices established and previously managed by Visa to ensure that software vendors and others develop secure payment applications that do not store sensitive card data.

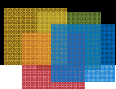
This white paper examines the requirements and ramifications of PA-DSS compliance as well as steps that VeriFone is taking to ease adoption.



---

## Content

Executive Summary	2
Ensuring Payment Security	Page 4
PA-DSS Overview	Page 5
PA-DSS Responsibilities	Page 6
PA-DSS Scope	Page 7
PA-DSS and Payment Terminals	Page 8
PA-DSS Ramifications	Page 9
VeriFone Implementation of PA-DSS	Page 10
Conclusion	Page 11



## Ensuring Payment Security

There is nothing more important than a consumer's trust in the payment system. Over the past two years, participants in the payment industry have forged a broad consensus around the need to ensure the security of electronic payment transactions and consistent application of requirements throughout the payments value chain to protect a consumer's identity and financial information.

The PCI SSC was founded by the five major international card brands—American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.—to consolidate and coordinate previously separate and overlapping efforts to establish enforceable security standards.

Those efforts have resulted in three sets of standards for which each of the card brands has incorporated into their data security compliance requirements and have implemented penalties for non-compliance:

- **PCI Data Security Standard (PCI DSS)** is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- **PCI PIN Transaction Security (PTS) Standard** provides security requirements, testing methodologies and approval information for vendors of Point of Interaction (POI) Terminals and Hardware Security Modules (HSM). This standard encompasses the earlier PCI PIN Entry Device (PED) requirements.
- **Payment Application Data Security Standard (PA-DSS)** is designed to help software vendors and others develop secure payment applications that do not store sensitive data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS.

PA-DSS requirements are derived from the PCI DSS and the PCI DSS Security Audit Procedures. This essentially codifies a set of best practices to ensure that software developers create applications that support the broader PCI DSS. At the time of its adoption, PA-DSS required all payment applications to be certified on a continuous basis using approved third-party security auditors known as Payment Application - Qualified Security Assessor (PA-QSA) laboratories.

### Glossary:

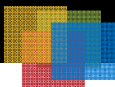
*PCI - Payment Card Industry*

*PCI SSC - PCI Security Standards Council*

*PCI DSS - PCI Data Security Standard*

*PA-DSS - Payment Application Data Security Standard*

*PABP - Payment Application Best Practices (Visa-formulated precursor to PA-DSS)*



## PA-DSS Overview

PA-DSS evolved from Visa's Payment Application Best Practices (PABP) to encompass any payment application which stores, processes, or transmits cardholder data as part of authorization or settlement, unless the application would fall under the merchant's PCI DSS validation.

PA-DSS encompasses retail and online payment application software. Its core goal is to help merchants comply with the requirements of PCI DSS as it applies to software.

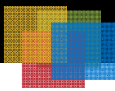
Since PCI DSS is a site compliance mandate for merchants that store, process, or transmit credit card data, it typically does not apply to payment application vendors unless they are providing a hosted solution.

However, according to PCI SSC, "since these payment applications are used by customers to store, process, and transmit cardholder data, and customers are required to be PCI Data Security Standard compliant, payment applications should facilitate, and not prevent, the customers' PCI Data Security Standard compliance."

PA-DSS validated applications, when used in a PCI DSS compliant environment, "will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches."<sup>i</sup>

According to PCI SSC, examples of how compliance with PCI-DSS can be compromised by payment applications include:

- Storage of sensitive authentication data after authorization—even if encrypted.
- Applications that require customers to disable other features required by the PCI Data Security Standard, like anti-virus software or firewalls, to get the payment application to work properly
- Vendor use of unsecured methods to connect to the application to provide support to the customer

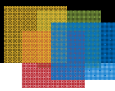


## PA-DSS Responsibilities

The PCI SSC maintains the PA-DSS guidelines and the card brands serve as the source of enforcement. Software vendors, acquirers and merchants are all charged with various responsibilities for compliance with PA-DSS.

**Payment application vendors** are responsible for ensuring, via a qualified review, that their applications “facilitate and do not prevent” PCI DSS compliance, creating implementation guides and educating their customers, resellers and integrators on how to install the applications in a compliant manner.

**Merchants and service providers, such as acquirers,** who purchase or otherwise obtain third-party payment applications, as well as resellers and integrators, are responsible for implementing them into a PCI DSS compliant environment and configuring according to the vendor’s PA-DSS Implementation Guide. Maintaining a PCI DSS compliant status of both the environment and the payment application is the responsibility of the merchant and the service provider.



## PA-DSS Scope

According to the PCI SSC, “a payment application is defined as one that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment applications is sold, distributed, or licensed to third parties.”

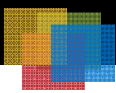
Specifically, this includes applications that are sold and installed “off the shelf” with little if any customization. It also applies to software that is provided in a modular fashion, with a “baseline” module and other modules that are specific to customer types or functions, or which are customized.

Excluded from the definition (but still subject to PCI DSS requirements) are:

- Operating systems, such as Windows and Unix, onto which a payment application is installed
- Database systems that store cardholder data
- Back-office systems that store cardholder data

Also excluded from PA-DSS are custom applications that are used by only one customer and designed and developed according to customer-provided specifications.

Another excluded category are in-house developed applications that are not sold, licensed or distributed to third parties. However, these in-house applications are still subject to the PCI DSS requirements for a secure environment.



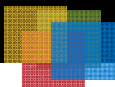
## PA-DSS and Payment Terminals

With the transition from Visa Payment Application Best Practices (PABP) to PA-DSS, the boundaries of the program expanded to include many POS terminal applications. Previously, under Visa's PABP, POS terminal applications were considered outside of the scope of the audit guidelines since the focus tended to center on PC-based applications.

This is an area that may be confusing to many, because PA-DSS excludes payment applications that are resident in standalone point-of-sale terminals provided that:

- The terminals have no connection to any of the merchant's systems or networks (i.e. integrated directly to an ECR or connected to an internal Ethernet or wireless network of multiple merchant PCs or ECRs)
- The terminals connect only to the merchant's acquirer or processor via a private line
- The payment application vendor provides secure remote updates, troubleshooting, access and maintenance
- Sensitive authentication data is never stored after authorization

The reality of the market, however, is that few terminals are likely to accommodate all of the restrictions that exclude them from PA-DSS. The overwhelming majority of "stand-alone POS terminal" payment applications being certified today by leading processors no longer meet all of these usage restrictions, so therefore fall under the scope of the PA-DSS compliance mandate.



## PA-DSS Ramifications

While there are exclusions to shield some non-custom payment applications from PA-DSS, the industry is rapidly moving to standardize on validated applications.

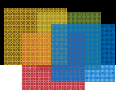
Also, Visa mandated, effective October 1st, 2008, that “Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or utilize PA-DSS compliant payment applications.”

Applications that have successfully completed a PA-DSS audit are certified to not retain or compromise what is considered to be secure elements of the card’s track data -- full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, and CVV2), PINs and PIN blocks.

Once a payment application has been validated by a qualified laboratory, even minor changes must be subsequently reviewed by a qualified assessor in order to ensure those changes do not negatively impact payment application security. If changes to the payment application do impact PA-DSS requirements, the payment application must undergo complete PA-DSS assessment.

It is important to note that reliance on PA-DSS validated payment applications do not alone guarantee PCI DSS compliance. The validated payment application must be implemented in a PCI DSS secure environment.

The only method of protecting your organization from card association penalties resulting from security breaches within your merchant portfolio is to strictly adhere to all card brand security mandates.



## VeriFone Implementation of PA-DSS

VeriFone applauds the PA-DSS standard as a bold step by industry regulators to mandate a validation testing program in an ongoing effort to keep criminals at bay. There is nothing more important than a consumer's trust in the payment system.

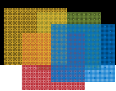
Our entire industry relies heavily on our collective ability to protect a consumer's identity and financial information. With VeriFone's significant market penetration, development and support infrastructure, the company is uniquely positioned to provide this important service to clients, who can pass this assurance onto their merchants and ultimately consumers.

The scope of PA-DSS requires an incremental step beyond our previous development and quality assurance process to ensure validation for every unique version of every application, for every acquirer, and in perpetuity.

This additional PA-DSS certification step comes at a high, but valuable cost to the industry due to the significant and ongoing certification fees that must be paid to the third-party PA-QSA laboratories that perform the validation assessments.

VeriFone was first in the industry to establish a comprehensive PA-DSS compliance policy aimed at ensuring protection of cardholder information across virtually all merchant environments and all types of card acceptance devices.

VeriFone adopted a universal compliance program for all of its applications used in its programmable payment acceptance devices going forward, initially targeting the US/Canada market. This includes the applications supporting the popular Vx and NuRIT product lines, which are both PA-DSS accepted. Auditing device-based payment applications at the supplier level minimizes the number of audits required and results in lower overall compliance costs for buyers.



## Conclusion

Payment security is a top priority for businesses today - across all industries and geographies. With card fraud always on the move and security standards changing so often, it's hard to keep up.

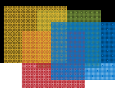
PA-DSS is a critical component to ensure successful compliance with the PCI Data Security Standard (PCI DSS). While large organizations may have the resources to monitor and implement compliance with all security mandates, there are millions of small- to mid-sized merchants with little ability to proactively protect their environments and their customers against increasingly sophisticated criminal efforts to obtain cardholder data.

Properly audited and PA-DSS accepted applications are a vital element in limiting exposure and liability for security breaches. As the leader in payments and payment security, VeriFone is aggressively taking steps to ensure new applications comply with security mandates.

Additional resources:

- [https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)
- [http://usa.visa.com/merchants/risk\\_management/cisp\\_payment\\_applications.html](http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html)
- [http://usa.visa.com/download/merchants/validated\\_payment\\_applications.pdf](http://usa.visa.com/download/merchants/validated_payment_applications.pdf)

For further information go to the PCI DSS section of the VeriFone web site at <http://www.verifone.com/about-us/industry-leadership/security/pci-dss.aspx>



Copyright © 2009 VeriFone. All rights reserved. No portion of this document may be reproduced or distributed in any form or by any means without the prior written permission of said company. All trademarks are the property of their respective owners

---

<sup>1</sup> PCI Security Standards Council LLC, PCI Payment Application Data Security Standard and Audit Procedures v1.1.