

ProStores PABP Implementation Guide - Store

Version 1.2

Prepared by: ProStores Inc., an eBay Company



Introduction

ProStores V9.X is compliant to the Visa Payment Application Best Practices (PABP) V1.4 and as such can be deployed successfully by customers in a Payment Card Industry Data Security Standard (PCI DSS) environment without violating any PCI criteria. This guide is designed to assist customers in such a deployment of ProStores Version 9.X in a PCI compliant manner.

ProStores Software is a web store building solution that provides hosting companies a platform that enables their small and medium sized merchants to sell products and services online through their own customizable virtual storefront. ProStores is available in four different store types:

Feature	Benefit	Starter	Business	Advanced	Enterprise
Easy-to-use Setup Wizard with professionally designed templates. Add your own company logo.	Get your store up and running in minutes.	✓	✓	✓	✓
Context-sensitive wizards that guide you through the setup process.	Complex tasks are presented in easy-to-use wizards with online help.	✓	✓	✓	✓
Extensive online help and printed documentation.	Save time performing tasks.	✓	✓	✓	✓
Upgrade easily and automatically from within store administration.	When you are ready to do more you can quickly and easily move to a more robust store building on your previous work.	✓	✓	✓	✓
eBay® integration.	Post products from your store to eBay for auction.	✓	✓	✓	✓
PayPal – real time payment acceptance and verification.	Accept real-time PayPal payments without investing in an online merchant account.	✓ ¹	✓ ¹	✓ ¹	✓ ¹
Additional payment options: major credit cards with real-time processing, store card, checks and money orders.	Accept additional forms of payment.	✓	✓	✓	✓
Shipping calculations based on order amount, order weight or total item count.	Create shipping tables to match your shipping needs.	✓	✓	✓	✓
Sophisticated tax calculations, including GST and PST for Canadian merchants.	Create sales tax calculations to match your sales tax needs	✓	✓	✓	✓
Customer profiles saved for quicker, friendlier check-out.	Shoppers profile saved so that they need not type it in every time they return to your store to purchase goods – saving the shopper time.	✓	✓	✓	✓

Feature	Benefit	Starter	Business	Advanced	Enterprise
Automated e-mail look up of lost passwords.	Shoppers can easily ask your store to provide them with their lost password – potentially reducing customer service calls.	✓	✓	✓	✓
Integrated shipping calculations: UPS®, FedEx®, United States Postal Service, and Canada Post.	Use UPS, FedEx, USPS or Canada Post shipping tables and tracking information similar to your retail business.	✓	✓	✓	✓
Intuitive, easy-to-use design tools that require no knowledge of HTML, allowing custom store design.	Customize your store design to match your corporate identity.		✓	✓	✓
Organize your catalog by category, product name, or manufacturer.	Categorize products in a fashion similar to your retail store – place products in multiple categories ensuring shoppers find the product they are looking for.		✓	✓	✓
Submit your products to multiple marketplaces including shopping search engines Yahoo! Shopping, Shopping.com, BizRate and Froogle. ³	Display your products in several shopping search engines, producing highly qualified traffic and an efficient sales channel for you		✓	✓	✓
Manage email marketing campaigns and newsletters with Constant Contact. ²	Create newsletters and email marketing campaigns to your shoppers.		✓	✓	✓
Share your product, order and customer information directly with QuickBooks®.	Easily share data with the most widely accepted accounting tool on the market – greatly reduces time spent on data entry		✓	✓	✓
Issue credits, partial credits and partial line item credits.	Easily credit a shopper for an incorrect order.		✓	✓	✓
Import & export of store data.	Easily import product and customer data, export customer and order data.		✓	✓	✓
Over a dozen reports to better manage your store.			✓	✓	✓
Advanced promotional capabilities including storewide sales, quantity discounts and promotion codes.	Increase traffic and return purchases by offering storewide sales, promotions for repeat shopping, etc.			✓	✓
Sophisticated inventory management tools.	Set inventory thresholds for reorders, display quantity in stock, hide out of stock inventory from storefront, allow shoppers to order backordered items.			✓	✓
Recurring billing lets you charge customers automatically at set intervals for products and services, such as monthly subscriptions.	Sell magazines, product of the month clubs, online subscriptions to content, etc and the store will automatically calculate the billing and charge at the intervals you define.			✓	✓

Feature	Benefit	Starter	Business	Advanced	Enterprise
Allow customers to download electronic products from your store.	Sell and deliver electronic goods like books, music, etc from your store.			✓	✓
Resale option.	Allow shoppers to purchase products resale and the store will automatically ask for the shopper's resale number and not charge them sales tax.			✓	✓
Add invoices via store administration.	Merchant can add invoices generated outside of online store – offer services and other non-tangible goods and/or input orders from mail/phone.			✓	✓
Additional payment options: purchase orders, internal department orders.	If selling to businesses, you can accept more advanced forms of payment similar to your offline business.			✓	✓
Adjust all elements up or down of an invoice ready for shipping.	Easily correct an order if a shopper over/under ordered.			✓	✓
Supply chain management: view pending orders by supplier, even if the order spans multiple suppliers; notify suppliers of orders electronically; provide suppliers secure area to update shipping status	Easily manage your supply chain and virtual inventory.				✓
Assign customers to different "buyer groups"	Manage wholesale, retail and frequent buyer groups from the same site. Shoppers will be displayed different product prices based on their login to the store.				✓
Create your own affiliate program	Let other sites sell your products – affiliates can link to your site, products, or cart with full reporting, variable commissions and online sign-up				✓
Gather sales leads by product	Gather shopper information on products that aren't for sale from the site but shoppers express an interest in – the store will automatically forward the information to a sales rep for follow-up				✓

1. PayPal processing fees apply.
2. These services are offered by third party vendors, additional fees may apply.

PABP requirements – general

This section will cover Store Administration settings that could have an impact on PCI compliance depending on how they are configured.

Customer - Store Administration settings

Store administrators should consider the following ProStores store administration settings when configuring their ProStores stores for PCI compliance:

- Store Settings – General
 - Security – Admin: Enable SSL for all administration pages. Only available if reseller/integrator has enabled this feature for store administration setting and has configured a SSL certificate. When enabled all store administration pages will be viewed via SSL including pages that include payment information and PAN. For PCI compliance it is recommended this setting be enabled.
- Store Settings – Payment Prefs
 - Credit Cards – Options: Retain customer credit card information. Only available if reseller/integrator has enabled this feature for store administration setting. Select this check box to indicate if customer credit card information should be saved. With this option enabled, returning customers will not have to reenter their credit card each time they purchase from your store. If you are not using a payment processor and you accept credit cards, you must enable this option in order to view payment details provided by the shopper and to complete processing of the order. If you are selling subscription or recurring billing goods, you must enable this option. For PCI compliance it is recommended that you only have this option enabled when the following conditions are met:
 - SSL has been enabled for Store Administration
 - User access to store administration areas that display full PAN is limited to those employees with a specific need to view this data. Review Section 2 of this document for details on setting user privileges.
 - Credit Cards – Options: Show credit card information within administration. Select this check box to display credit card numbers in the Customer Profile and Orders Pending Credit Card Authorization list. If you will be processing payment offline or it is necessary to review payment details, you need to select this check box so that the information is available for review or entry into your terminal. For PCI compliance it is recommended that you only have this option enabled when the following conditions are met:
 - SSL has been enabled for Store Administration
 - User access to Customer Profile and Orders Pending Credit Card Authorization pages in store administration is limited to those employees with a specific need to view this data. Review Section 2 of this document for details on setting user privileges.
 - Storewide Preferences – Security: Enable SSL on order process. Only available if reseller/integrator has enabled this feature for store administration setting. Select this check box to enable SSL during the order process. When the customer begins the checkout process, all activity through order confirmation will be SSL protected. You must have an SSL certificate installed to use this feature. For PCI compliance it is required that you have this option enabled.
- Store Design – Template Management

- Merchants can control the design of their storefront including the addition of custom HTML, JavaScript or other design commands from within Store Administration. Merchants are fully responsible for the management of the content that appears in their storefronts. As such, Merchants should limit the access to this function of store administration to only those personnel with a need to customize store design. All code should be reviewed prior to loading onto templates to ensure that the security of the storefront is not being compromised. Merchants should take care and perform periodic audits of all storefront templates to ensure that they are following all PABP and PCI best practices.
- Product Manager – Add / Update Product Information
 - Merchants can control the descriptions of their products including the addition of custom HTML, JavaScript or other design commands from within Store Administration when creating or updating product descriptions. Merchants are fully responsible for the management of the content that appears in their storefronts. As such, Merchants should limit the access to this function of store administration to only those personnel with a need to customize product descriptions. All code should be reviewed prior to loading into product fields that allow markup to ensure that the security of the storefront is not being compromised. Merchants should take care and perform periodic audits of product fields to ensure that they are following all PABP and PCI best practices.
- Category Manager – Add / Update Category Information
 - Merchants can control the descriptions of their categories including the addition of custom HTML, JavaScript or other design commands from within Store Administration when creating or updating category descriptions. Merchants are fully responsible for the management of the content that appears in their storefronts. As such, Merchants should limit the access to this function of store administration to only those personnel with a need to customize category descriptions. All code should be reviewed prior to loading into category fields that allow markup to ensure that the security of the storefront is not being compromised. Merchants should take care and perform periodic audits of category fields to ensure that they are following all PABP and PCI best practices.

PABP Section 2 requirements

It is possible for Store Administrators of ProStores to set permissions that allow store personnel to see the full credit card number and corresponding expiration date if the functionality has been enabled by the ProStores reseller/integrator.

Customer - Store Administration User Settings

Store administrators can control access to their ProStores Store Administration by managing users with different permission levels. This is found in Store Administration, Store Settings – Users. Care should be taken when providing store administrators access rights to ProStores Store Administration, specifically access to Store Settings Manager, Order Manager (and its child privileges of Order Manager – Order Authorization and Order Manager – Order Entry), and Customer Manager (and its child privileges of Customer Manager – Store Credit). Only those employees with a need to see full PAN or configure store settings for the storage and viewing of credit card data should be granted access rights to these areas of Store Administration. It is recommended that different users be created with different permissions based on their need to access Store Administration functions.

It is the Customers responsibility to institute proper personnel management techniques for allowing administrative user access to credit cards, site data, and all other aspects of store administration. In most situations, security breach is the result of unethical personnel. So pay

special attention to whom you trust into your store administration area and who you allow access to sensitive customer data.

PABP Section 3 requirements

Password requirements and management

For PCI compliance, the following user authentication and password management for System and Store Administration users is required (per PCI Data Security Standard 8.5.9 through 8.5.15) – this is controlled natively within ProStores for Store Administration (version 9.2 and above):

- Do not use group, shared, or generic accounts and passwords
- Change user passwords at least every 90 days
- Require a minimum password length of at least seven characters
- Use passwords containing both numeric and alphabetic characters
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- Limit repeated access attempts by locking out the user ID after not more than six attempts
- Set the lockout duration to thirty minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

In addition, the following should be noted:

Customers are

- advised against using administrative accounts for application logins as explained in detail in PABP Section 2 requirements, above.
- advised to assign strong passwords to these default accounts even if they won't be used, and then disable or do not use the accounts. ProStores will natively require password management meet the above requirements however it is recommended that the customer take care to ensure strong passwords are assigned to other applications and systems whenever possible
- advised to assign strong application and system passwords whenever possible to other systems outside of ProStores. PCI compliance requires password and management strength meet the requirements stated above
- advised to control access, via unique username and PCI DSS-compliant complex passwords (described above), to any PCs, servers, and databases with payment applications and cardholder data

PABP Section 6 requirements

Wireless Access

While not configurable within the ProStores application and not recommended or supported by ProStores, organizations installing ProStores within a wireless environment and wishing to maintain their PCI compliance must comply with the following guidelines:

- Corporate mobile devices and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the

organization's network, have personal firewall software installed and active, which is configured by the organization to specific standards and not alterable by the employee

- Ensure that all of the default vendor settings are changed. For example, ensure any SSID value, SNMP Community strings, and administrative passwords are changed from default.
- Access points must utilize the Wi-Fi Protected Access (WPA or WPA-2) protocols to meet PCI version 1.2 Requirements. Use of the Wired Equivalent Privacy (WEP) security protocol does not meet PCI requirements, and must not be employed.
- Ensure the SSID has been changed from the default setting, and that the broadcast of the SSID has been disabled.
- All wireless networks that transmit cardholder data or that are connected to cardholder environments must utilize PCI compliant encryption technologies, such as: Wi-Fi Protected Access (WPA or WPA2), IPSEC VPN, or SSL/TLS.

Additional details on compliance for wireless networks may be found in the PCI Data Security Standard 1.3.9, 2.1.1 and 4.1.1.

PABP Section 9 requirements

Cardholder Data Storage

In order to comply with PCI requirements, Customers should not perform actions that would copy, transmit or store cardholder data onto separate Internet accessible servers.

PABP Section 11 requirements

Remote Access (Cont.)

The ProStores application may be configured in a number of ways. In order to ensure the application is installed in a PCI compliant manner, ensure:

- Access to Store Administration areas are only accessible using the HTTPS protocol and a valid SSL certificate.
- Ensure each user of the application is provided unique credentials.
- Ensure default settings in any remote access application are modified (such as default user names / passwords)
- Restrict remote access to the application to known source IP/ MAC addresses and protocols.
- Remote access to the hosting environment for administration purposes must be performed using 2-factor authentication.
- Enforce strong authentication or complex passwords for login credentials (according to PCI DSS requirements 8.1, 8.2, 8.4, 8.5.).
- Enforce encryption of data between the application and the remote client.
- Enable account lockout after failed login attempts.
- Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access to the application is allowed.
- Enable all logging functions.

PABP Section 12 requirements

ProStores allows data transmission over the Internet and thus recommends that customers have SSL installed and configured for their ProStores environments. ProStores does not facilitate the sending of credit card information (PAN) by email. Customers should not send PANs by email unless they are encrypted using an email encryption program such as PGP.

Customer – SSL Configuration and Settings

Customers should work with their ProStores reseller/integrator to install SSL for their stores, whether shared or dedicated for their unique store URL. Once installed by the reseller/integrator the customer should configure the following settings in Store Administration in order to comply with Section 4.1 of the PCI Data Security Standard:

- Store Settings – General
 - Security – Admin: Enable SSL for all administration pages. Only available if reseller/integrator has enabled this feature for store administration setting and has configured a SSL certificate. When enabled all store administration pages will be viewed via SSL including pages that include payment information and PAN. For PCI compliance it is recommended this setting be enabled.
- Store Settings – Payment Prefs
 - Storewide Preferences – Security: Enable SSL on order process. Only available if reseller/integrator has enabled this feature for store administration setting. Select this check box to enable SSL during the order process. When the customer begins the checkout process, all activity through order confirmation will be SSL protected. You must have an SSL certificate installed to use this feature. For PCI compliance it is required that you have this option enabled.

PABP Section 13 requirements

ProStores allows data transmission over the Internet and thus recommends that Customers have SSL installed and configured for their ProStores environments. Please review PABP Section 12 requirements for details on SSL configuration and settings.

PABP Section 14 requirements

This guide is disseminated to all relevant application users as a pdf file downloadable from ProStores website – customers can download the document from ProStores Learning Center at <http://learningcenter.prostores.com>.

This guide covers all sections as required by the PABP standard and is subject to annual review, with updates for changes to software and for changes to the requirements in this document.