PAYware Connect Integration Best Practices

Users and Passwords

Important Security Notice

Payment Card Industry (PCI) Security Standard

Introduction and Scope

The Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS) is comprised of fourteen requirements that support the Payment Card Industry Data Security Standard (PCI DSS). The PCI Security Standards Council (PCI SSC), which was founded by the major card brands in June 2005, set these requirements in order to protect cardholder payment information. The standards set by the council are enforced by the payment card companies who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.

PCI PA-DSS is an evolution of Visa’s Payment Application Best Practices (PABP), which was based on the Visa Cardholder Information Security Program (CISP). In addition to Visa CISP, PCI DSS combines American Express’ Data Security Operating Policy (DSOP), Discover Network’s Information Security and Compliance (DISC), and MasterCard’s Site Data Protection (SDP) into a single comprehensive set of security standards. The transition to PCI PA-DSS was announced in April 2008. In early October 2008, PCI PA-DSS Version 1.2 was released to align with the PCI DSS Version 1.2, which was released on October 1, 2008. On January 1, 2011, PCI PA-DSS Version 2.0 was released. This extends the PCI DSS Version 1.2, which was released on October 1, 2008 and is effective as of January 1, 2011.

1. Sensitive Data Storage Guidelines.

Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data.

   1.1 Do not store sensitive authentication data after authorization (even if encrypted):

       Sensitive authentication data includes the data as cited in the following Requirements 1.1.1 through 1.1.3.

       PCI Data Security Standard Requirement 3.2

       Note: By prohibiting storage of sensitive authentication data after authorization, the assumption is that the transaction has completed the authorization process and the customer has received the final transaction approval. After authorization has completed, this sensitive authentication data cannot be stored.

       1.1.1 After authorization, do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
PAYware Connect Best Practices
Users and Passwords
Updated October 14, 2011

In the normal course of business, the following data elements from the magnetic stripe may need to be retained:

- The accountholder’s name,
- Primary account number (PAN),
- Expiration date, and
- Service code
- To minimize risk, store only those data elements needed for business.

**Note:** See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information. PCI Data Security Standard Requirement 3.2.1

1.1.2 After authorization, do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.

**Note:** See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information. PCI Data Security Standard Requirement 3.2.2

1.1.3 After authorization, do not store the personal identification number (PIN) or the encrypted PIN block.

**Note:** See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information. PCI Data Security Standard Requirement 3.2.3

1.1.4 Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.

**Note:** This requirement only applies if previous versions of the payment application stored sensitive authentication data.

1.1.5 Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINs or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use. PCI Data Security Standard Requirement 3.2

2. Protect stored cardholder data

2.1 Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period. PCI Data Security Standard Requirement 3.1

2.2 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

**Notes:**

- This requirement does not apply to those employees and other parties with a legitimate business need to see full PAN;
- This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts. PCI Data Security Standard Requirement 3.3
2.3 Render PAN, at a minimum, unreadable anywhere it is stored, (including data on portable digital media, backup media, and in logs) by using any of the following approaches:
   • One-way hashes based on strong cryptography with associated key management processes and procedures
   • Truncation
   • Index tokens and pads (pads must be securely stored)
   • Strong cryptography with associated key management processes and procedures.
The MINIMUM account information that must be rendered unreadable is the PAN. PCI Data Security Standard Requirement 3.4

The PAN must be rendered unreadable anywhere it is stored, even outside the payment application.
Note: “Strong cryptography” is defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.

2.4 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts. PCI Data Security Standard Requirement 3.4.2

2.5 Payment application must protect cryptographic keys used for encryption of cardholder data against disclosure and misuse. PCI Data Security Standard Requirement 3.5

2.6 Payment application must implement key management processes and procedures for cryptographic keys used for encryption of cardholder data. PCI Data Security Standard Requirement 3.6

2.7 Securely delete any cryptographic key material or cryptogram stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations. These are cryptographic keys used to encrypt or verify cardholder data. PCI Data Security Standard Requirement 3.6

Note: This requirement only applies if previous versions of the payment application used cryptographic key materials or cryptograms to encrypt cardholder data.

3. Provide secure authentication features

3.1 The payment application must support and enforce unique user IDs and secure authentication for all administrative access and for all access to cardholder data. Secure authentication must be enforced to all accounts generated or managed by the application by the completion of installation and for subsequent changes after the “out of the box” installation (defined at PCI DSS Requirements 8.1, 8.2, and 8.5.8-8.5.15) for all administrative access and for all access to cardholder data. PCI Data Security Standard Requirements 8.1, 8.2, and 8.5.8-8.5.15

Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the payment application. This requirement applies to the payment application and all associated tools used to view or access cardholder data.
PAYware Connect Best Practices
Users and Passwords
Updated October 14, 2011

3.1.10 If a payment application session has been idle for more than 15 minutes, the application requires the user to re-authenticate. PCI Data Security Standard Requirement 8.5.15.

3.2 Software vendors must provide guidance to customers that all access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication. PCI Data Security Standard Requirements 8.1 and 8.2

3.3 Render payment application passwords unreadable during transmission and storage, using strong cryptography based on approved standards

Note: “Strong cryptography” is defined in PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms. PCI Data Security Standard Requirement 8.4

4. Log payment application activity

4.1 At the completion of the installation process, the “out of the box” default installation of the payment application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users. PCI Data Security Standard Requirement 10.1

4.2 Payment application must implement an automated audit trail to track and monitor access. PCI Data Security Standard Requirements 10.2 and 10.3

5. Develop secure payment applications

5.1 Develop all payment applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices and incorporate information security throughout the software development life cycle. These processes must include the following: PCI Data Security Standard Requirement 6.3

5.1.1 Live PANs are not used for testing or development. PCI Data Security Standard Requirements 6.4.4.

5.1.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)
5.1.1.2 Validation of proper error handling
5.1.1.3 Validation of secure cryptographic storage
5.1.1.4 Validation of secure communications
5.1.1.5 Validation of proper role-based access control (RBAC)

5.1.2 Separate development/test, and production environments
5.1.3 Removal of test data and accounts before production systems become active development. PCI Data Security Standard Requirement 6.4.4.
5.1.4 Review of payment application code prior to release to customers after any significant change, to identify any potential coding vulnerability. Removal of custom payment application accounts, user IDs, and passwords before payment applications are released to customers.

Note: This requirement for code reviews applies to all payment application components (both internal and public-facing web applications), as part of the system development life cycle required by PA-DSS Requirement 5.1 and PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties.
5.2 Develop all web payment applications (internal and external, and including web administrative access to product) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include:

5.2.1 Injection flaws, with particular emphasis on SQL injection, Cross-site scripting (XSS) OS Command Injection, LDAP and Xpath injection flaws, as well as other injection flaws.
5.2.2 Buffer Overflow.
5.2.3 Insecure cryptographic storage.
5.2.4 Insecure communications.
5.2.5 Improper error handling.
5.2.6 All “HIGH” vulnerabilities as identified in the vulnerability identification process at PA-DSS Requirement 7.1.
5.2.7 Cross-site scripting (XSS)
5.2.8 Improper access control such as insecure direct object references, failure to restrict URL access and directory traversal.
5.2.9 Cross-site request forgery (CSRF)

Note: The vulnerabilities listed in PA-DSS Requirements 5.2.1 through 5.2.9 and in PCI DSS at 6.5.1 through 6.5.9 were current in the OWASP guide when PCI DSS v1.2 / PCI DSS v2.0 (01/01/10) were published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.

5.3 Software vendor must follow change control procedures for all product software configuration changes. PCI Data Security Standard Requirement 6.4.5. The procedures must include the following:

5.3.1 Documentation of impact
5.3.2 Management sign-off by appropriate parties
5.3.3 Testing functionality to verify the new change(s) does not adversely impact the security of the system. Remove all testing configurations, samples, and data before finalizing the product for production.
5.3.4 Back-out or product de-installation procedures

5.4 The payment application must not use or require use of unnecessary and insecure services and protocols (for example: NetBIOS, file-sharing, Telnet, unencrypted FTP must be secured via SSH, S-FTP, SSL, IPSec and other technology to implement end to end security). PCI Data Security Standard Requirement 2.2.2

6. Protect wireless transmissions

6.1 For payment applications using wireless technology, the wireless technology must be implemented securely. Change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. The end to end wireless implementation must be secure. PCI Data Security Standard Requirements 1.2.3 & 2.1.1

6.2 For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Payment applications using wireless technology must facilitate the following regarding use of WEP*: PCI Data Security Standard Requirement 4.1.1

* The use of WEP as a security control was prohibited as of 30 June 2010.
PAYware Connect Best Practices
Users and Passwords
Updated October 14, 2011

7. Test payment applications to address vulnerabilities

7.1 Software vendors must establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet) and to test their payment applications for vulnerabilities. Any underlying software or systems that are provided with or required by the payment application (for example, web servers, third-party libraries and programs) must be included in this process. Remove all test configurations, samples, and data after testing and before promoting the changes to production. PCI Data Security Standard Requirement 6.2

7.2 Software vendors must establish a process for timely development and deployment of security patches and upgrades, which includes delivery of updates and patches in a secure manner with a known chain-of-trust, and maintenance of the integrity of patch and update code during delivery and deployment.

8. Facilitate secure network implementation

8.1 The payment application must be able to be implemented into a secure network environment. Application must not interfere with use of devices, applications, or configurations required for PCI DSS compliance (for example, payment application cannot interfere with anti-virus protection, firewall configurations, or any other device, application, or configuration required for PCI DSS compliance). PCI Data Security Standard Requirements 1, 3, 4, 5, and 6.

9. Cardholder data must never be stored on a server connected to the Internet

9.1 The payment application must be developed such that the database server and web server are not required to be on the same server, nor is the database server required to be in the DMZ with the web server. PCI Data Security Standard Requirement 1.3.7

10. Facilitate secure remote software updates

10.1 If payment application updates are delivered securely via remote access into customers’ systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure authentication using a two factor authentication mechanism. PCI Data Security Standard Requirement 8.3

10.2 If payment application may be accessed remotely, remote access to the payment application must be authenticated using a two factor authentication mechanism. PCI Data Security Standard Requirement 8.3

10.3 Any remote access into the payment application must be done securely. If vendors, resellers/integrators, or customers can access customers’ payment applications remotely, the remote access must be implemented securely. PCI Data Security Standard Requirements 1, 8.3 and 12.3.9

11. Encrypt sensitive traffic over public networks

11.1 If the payment application sends, or facilitates sending, cardholder data over public networks, the payment application must support use of strong cryptography and security protocols such as SSL/TLS and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.
Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

PCI Data Security Standard Requirement 4.1

11.2 The payment application must never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, and chat). PCI Data Security Standard Requirement 4.2

12. Encrypt all non-console administrative access

12.1 Instruct customers to encrypt all non-console administrative access using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. Telnet or remote login must never be used for administrative access. PCI Data Security Standard Requirement 2.3

13. Maintain instructional documentation and training programs for customers, resellers, and integrators

13.1 Develop, maintain, and disseminate a PA-DSS Implementation Guide(s) for customers, resellers, and integrators that accomplishes the following:

13.1.1 Addresses all requirements in this document wherever the PA-DSS Implementation Guide is referenced.

13.1.2 Includes a review at least annually and updates to keep the documentation current with all major and minor software changes as well as with changes to the requirements in this document.

13.2 Develop and implement training and communication programs to ensure payment application resellers and integrators know how to implement the payment application and related systems and networks according to the PA-DSS Implementation Guide and in a PCI DSS-compliant manner.

13.2.1 Update the training materials on an annual basis and whenever new payment application versions are released.

PAYware Connect Username and Password Settings

Username Requirement

- Maximum length of eight characters for Merchant Users - this field is not case-sensitive
- If you have not yet created a user, there should only be one user shown in the User Table under Account Admin in the Virtual Terminal. This is the default Administrator level user provided to you when you subscribed to this payment processing service.

***We recommend that this main Administrator level user ID not be used for general transactions.
PAYware Connect Best Practices
Users and Passwords
Updated October 14, 2011

Password Requirements
- Must be minimum of eight alpha/numeric characters in length and maximum of 14 alpha/numeric characters in length
- Must differ from the previous six password submissions
- Must be case sensitive
- Must contain at least three upper case characters
- Must contain at least two numeric characters
- Must not contain repeating characters of the same case and/or numeric value (e.g., AA, aa, 22)
- Must not contain any group of 3 sequential numbers or characters within the same case (e.g., 234, fgh, ABC, etc.)

Password Expiration - (Implemented 06/09/2008)
- When using the Virtual Terminal to access the PAYware Connect Merchant Console, passwords will expire after 90 days, including a 10 day warning period
- When processing transactions through integration using the PAYware Connect API, this password expiration will not occur - provided the merchant does NOT attempt to log into the Virtual Terminal. At this point, the user will have to change his/her password as well as update it in the payment application processing through PAYware Connect.

Account Lockout
- Your user ID will be temporarily locked if there are three unsuccessful login attempts. The lockout time is 30 minutes.
- If the account is locked out for the incorrect password automatically by PAYware Connect. After remaining locked out for 30 minutes, it will automatically become reinabled.
- The Merchant or Reseller can also reactive the account immediately once the lockout reason is understood. These Merchant or Reseller Users must have privileges to access the User Manager on the account in order to unlock the username.
- If you are an Administrator user and have been locked out of your account, you must either call your PAYware Connect Reseller or wait 30 minutes for the account to unlock. If you cannot contact your PAYware Connect Reseller, you may contact PAYware Connect Technical Support.

Lost or Forgotten Passwords
- If you lose your Administrator password, it must be reset by your PAYware Connect Reseller. PAYware Connect passwords are encrypted and cannot be retrieved—a new password must be generated. If you cannot contact your PAYware Connect Reseller, you may contact PAYware Connect Technical Support.
- If you receive a newly generated password, you must change it immediately upon login. Once the password is changed via the User Manager in the Virtual Terminal.
Username and Password Best Practices for Integrators

VeriFone Recommendations

• The Merchant/Integrator must ensure that the password passed by application using the API (USER_PW) is the current Password that is configured in PAYware Connect.

• The Merchant/Integrator must also ensure that the Username that is passed by the application using the API (USER_ID) is currently active on that merchant’s account.

• It is the Merchant’s responsibility to change the password used by the API on a regular basis. PAYware Connect will only require Virtual Terminal access users to change every 90 Days.

• The USER_ID used by the API should also be restricted by the Merchant/Reseller to only have the Role and Permissions required to process transactions via the API. This means that the API USER_ID should NOT have Administrator rights and should NOT have the ability to setup new users or run transactions that HAVE not been authenticated with the API Application. Failure to do follow these recommendations will open a security gap in the Merchant’s account and provide anyone that has access to the API/Application configuration to have unrestricted access to the Merchant account.

• If the Merchant or Reseller changes the User Password, it must immediately be changed on the API interface to match what has been set up on the merchant’s account or no further transactions will be authenticated through the API to be processed. The USER_ID/USER_PW must always match what is sent in the API Transaction to the current Password in PAYware Connect.

• Merchants and Resellers should setup separate Usernames used for Integration versus Virtual Terminal Access.

Summary of Recommendations

• Integrators that currently have integrated a USER_ID/USER_PW for a specific Merchant Account, this USER_ID should remain dedicated to the API and not utilized by any individual for Virtual Terminal access. This will prevent any user from changing the password and preventing the API transactions from processing.

• Integrators/Merchants should setup unique username for Virtual Terminal access. These users should have the required Role/Permissions that user is authorized to have in regards to business needs and processing needs. This username and password for PCI DSS compliance should not be shared or used by any other individual. The Password will also be required to be changed on a regular basis through the Virtual Terminal.

• On a regular basis, determined by the Merchant/Reseller, the USER_PW used by the API Application should be changed to prevent the merchant’s account from becoming compromised by allowing unauthorized access. The
PAYware Connect Best Practices
Users and Passwords
Updated October 14, 2011

password in PAYware Connect and used through the API in the integrated application should be updated in parallel.

** If properly executed, there should be NO NEGATIVE IMPACT to any integrated application due to password expiration requirements only enabled by accessing the Virtual Terminal. These password expiration requirements are mandated for PCI DSS compliance. They are intended to protect cardholder data, the Merchant and Reseller Accounts, and ensure VeriFone is able to offer a PCI DSS Complaint Service to our customers.

For further information on PCI Data Security Standards, visit [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org).

Contact Information

Mailing Address

VeriFone, Inc.
8001 Chatham Center Drive
Suite 500
Savannah, GA 31405

Telephone

Savannah Sales Office: (800) 725-9264
Savannah Office Fax: (912) 527-4533

Web Site

[www.verifone.com](http://www.verifone.com)