PayLINK

Implementation Guide

PayLINK Implementation Guide

Version 2.1.252

Released September 17, 2013

Table of Contents

Chapter 1. Overview 5
1.1. Purpose of this document 5
1.2. What are PCI and PA-DSS 5
1.3. PA-DSS Scope... 5
Chapter 2. PA-DSS Requirements...7
2.1. Overview.. 7
2.2. Managing Customer Data for Support & Troubleshooting Activities 8
2.3. Provide Secure Authentication Features... 9
2.4. Log Application Activity 9
2.5. Always Use Secure Coding Guidelines... 10
2.6. Protect Wireless Transmissions.. 10
2.7. Test Applications to Identify and Address Security Vulnerabilities.................................. 11
2.8. Facilitate Secure Network Implementations.. 11
2.9. Cardholder Data Should Never Be Seen or Stored on a Internet-connected Server 11
2.10. Facilitate Secure Remote Software Updates.. 12
2.11. Facilitate Secure Remote Access to the Application 12
2.12. Encrypt Sensitive Traffic Over Public Networks 13
2.13. Encrypt All Non-Console Administrative Access 13
2.14. Maintain Instructional Documentation and Training Programs for Customers.............. 13
2.15. Additional Information 13

Changes and Modifications

The table below lists changes made to the PayLINK Implementation Guide:

Version	Changes/Modifications	Pages
1.0	Document launch.	All
2.0	Updated format for release 251; Removed addendum.	All
2.1.252	Updated version information for release 252.	All

Chapter 1. Overview

1.1. Purpose of this document

This document provides a list of PA-DSS requirements for the application vendor implementing the PayLINK integration and spells out the responsibilities for the application vendor to ensure their application meets the Payment Application Data Security Standards (PADSS).

The PayLINK Implementation Guide will be reviewed and updated anytime there are changes to our applications that affect PA-DSS or the application's implementation. This document will be reviewed no less than annually. Developers are strongly encouraged to check this document annually to verify if there have been any changes.

1.2. What are PCI and PA-DSS

Systems that process electronic payment transactions necessarily handle sensitive cardholder account information. The Payment Card Industry (PCI) has developed security standards for handling cardholder information called the PCI Data Security Standard (DSS). These security requirements defined in the DSS apply to all members, merchants, application and service providers that store, process, or transmit cardholder data.

Payment Application Data Security Standards (PA-DSS) apply to software vendors who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement. Payment applications, when implemented according to PA-DSS and when implemented into a PCI DSS-compliant environment, should facilitate and support customers' PCI DSS compliance.

Compliance validation for PA-DSS has taken place in the PayLINK solution thus avoiding the need for the software vendor to incur the time and expense to complete PA-DSS certification provided they adhere to the requirements outlined in this implementation guide. This approach allows the application developer to focus on creating user experiences and business logic while PayLINK takes care of the PA-DSS functionality.

1.3. PA-DSS Scope

By using the PayLINK solution, the software vendor never sees, stores, processes, or transmits cardholder data. Thus, the software vendor is not required to have the application PA-DSS certified, as long as they follow the requirements outlined in this implementation guide and **NEVER** see, store, process, or transmit cardholder data---period.

Examples of applicable payment applications include, but are not limited to, point-of-sale (POS) software, e-Commerce shopping carts, and Web based payment applications if they store, process, or transmit cardholder data. PA-DSS does not apply to payment applications that are developed by merchants and agents if the application is only used in-house (not sold or distributed to a third party). PA-DSS also does not apply to standalone POS terminals that meet the following conditions:

- The terminal has no connections to any of the merchant's systems or networks
- The terminal connects to the acquirer or processor
- The terminal vendor provides secure remote updates, troubleshooting, access, and maintenance
- The following are never stored after authorization: the full contents from the magnetic stripe (that is on the back of a card, in a chip, or elsewhere), PAN, CVV, CVV2, PIN or encrypted PIN block

For more information, visit the Payment Card Industry Security Standards Council Web site at https://www.pcisecuritystandards.org.

Chapter 2. PA-DSS Requirements

2.1. Overview

The following sections outline the specific PA-DSS requirements for the application vendor.

Applications must enforce the unique login requirements prescribed by PA-DSS. An application must require unique user names and complex passwords for all administrative access and for all access to data center and meet PA-DSS security requirements:

- 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 no 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

Customer's note:

- You are advised ***against*** using administrative accounts for application logins.
- You are 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.
- You are advised to ***assign strong application and system passwords*** whenever possible to other systems outside of PayLINK.
- 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.

PayLINK does not provide or persist any sensitive cardholder transaction data to the vendor's application. Sensitive cardholder data includes:

- Magnetic stripe data

- Card validation values or codes
- PINs
- PIN block data
- PAN (Primary Account Number)

Application developer's note:

- Changing the "out of the box" installation settings for unique user IDs and secure authentication will result in merchant non-compliance with PCI DSS.

An application should use PayLINK to process the transaction and must not provide any inputs for cardholder data (manual or swiped) and consequently must not see or store the cardholder data including the full contents of any track from the magnetic stripe on the back of the card, the card validation value (CVV/CVV2/CID), or the PIN (or encrypted PIN block) anywhere, including in any of the components below.

- Transaction logs
- History files
- Trace files
- Debugging and error logs
- Audit logs
- Database schemas and tables
- Database contents

Since PayLINK does not store any cardholder data, it becomes the customer's responsibility for purging any sensitive cardholder data stored outside of PayLINK. This applies to (PAN alone or with any of the following: expiration date, cardholder name or service code):

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period must be purged.

2.2. Managing Customer Data for Support & Troubleshooting Activities

Since the application developer never sees sensitive cardholder data, a reference token is returned by PayLINK to provide access to transaction information that is stored in a secure PCI certified data center.

The offsite PCI certified data center secures data by implementing tokenization and encryption techniques in a nearly transparent process. Tokenization is the process of substituting a value in place of sensitive information. The token doesn't retain any relationship to the information in which it is substituted; it is not masked or encrypted, so there is no means to hack or solve the missing piece. Instead the token is a key to access the information that resides in a physically separate location, also referred to as offsite cardholder data storage. This ensures that if a merchant should suffer a security breach, cardholder data is omitted from the compromised information.

2.3. Provide Secure Authentication Features

To use PayLINK, you must provide a principal user name and login credential for the Payment Gateway. For administrative users, the credential must be a secure, PA-DSS-compliant password. Passwords must be a minimum of seven characters, at least one of which must be a number or non-alphanumeric. Passwords must also be rotated every 90 days, and the last four versions must be unique (i.e., cannot be repeats of any of the last four passwords used).

Access for non-administrative users can be provided with a user name and token, instead of a password. The use of non-expiring tokens is only permissible for users that do not have access to cardholder data and other features that are restricted to administrative users.

PayLINK verifies the complexity level of the provided password and provides a warning or rejects it if it does not meet the minimum requirements.

2.4. Log Application Activity

At the completion of the installation process, PayLINK logs all user access (especially users with administrative privileges), and is able to link all activities to individual users. PayLINK also implements an automated audit trail to track and monitor access.

Specifically, the audit trails must be suitable to reconstruct the following events:

- All individual access to cardholder data
- All actions taken by administrative users
- Access to the audit trails themselves
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

Additionally, the following elements must be logged by the payment application for each event:

- User identification
- Type of event
- Date and time
- Success or failure indication

- Origination of event
- Identity or name of affected data, system component, or resource

PayLINK logging is enabled automatically**. *Disabling or in any way tampering with*** application logging should not be done and ***will result in merchant non-compliance with PCI DSS*.**

2.5. Always Use Secure Coding Guidelines

This requirement is outside of the scope of PayLINK and is up to the application developer to implement manually, if applicable.

At a minimum, when developing a Web-based application, the software development process must follow standard guidelines and include appropriate training for the development team. Processes must be in place to ensure that applications are not at risk to the common coding vulnerabilities specified in PCI Data Security Standard 6.5.

2.6. Protect Wireless Transmissions

This requirement is outside of the scope of PayLINK. If the vendor’s application can be implemented in a wireless environment, the application must not prevent the following wireless requirements from being met and the application's PA-DSS Implementation Guide must contain the following guidance to customers:

- For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to, default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission. Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example, AES):
- Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions.
- Default SNMP community strings on wireless devices were changed.
- Default passwords/passphrases on access points were changed.
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2).
- Other security-related wireless vendor defaults, if applicable.
- Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such access is required for business purposes) any traffic from the wireless environment into the cardholder data environment.

- Ensure wireless networks transmitting cardholder data, or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
- For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.
- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

2.7. Test Applications to Identify and Address Security Vulnerabilities

This requirement is outside of the scope of PayLINK. The testing and development process should include a process to identify newly discovered security vulnerabilities and to develop and deploy security patches and upgrades in a timely manner. Updates and patches must be delivered in a secure manner with a known chain-of-trust. Any underlying software or systems that are provided along with the application (e.g., Web servers) must be included in this process.

In addition, customers should be recommended to subscribe to one of the alert services freely available on the Internet to ensure they are not exposed to risk.

It is always recommended to install all Microsoft updates as soon as they are released on all computers where PayLINK is installed. The type of Microsoft updates that should be installed are those classified by Microsoft as Security Updates, Critical Updates, Service Packs, Important Updates, and Recommended updates. It is important to install updates as soon as possible once they are released and always within 30 days of release.

In order to be aware of new updates from Microsoft, PayLINK suggests that all vendor applications subscribe to an industry standard vulnerability advisory service such as the SANS@RiskNewsletter found at the following URL: http://www.sans.org/newsletters/risk/.

2.8. Facilitate Secure Network Implementations

This requirement is outside of the scope of the PayLINK. Customers must be able to implement an application into a secure network environment. Applications must not interfere with use of network address translation (NAT), port address translation (PAT), traffic filtering network devices, anti-virus protection, patch or update installation, or encryption.

2.9. Cardholder Data Should Never Be Seen or Stored on an Internet-connected Server

PA-DSS states that payment applications must not require that the database server and Web server be on the same server, or in the DMZ with the Web server.

PayLINK does NOT store any sensitive cardholder data (including data from the magnetic stripe or PAN) on the server where it is running with the integrated POS application, NOR does PayLINK return any sensitive cardholder data to the integrated application.

2.10. Facilitate Secure Remote Software Updates

This requirement is outside the scope of PayLINK. If software and updates are delivered via remote access, customers must be aware of the following:

Customers should turn on their modem only when needed for downloads and turned off immediately after download completes.

If the computer is connected via VPN or other high-speed connection, customers should use a personal firewall product to secure these "always-on" connections

2.11. Facilitate Secure Remote Access to the Application

This requirement is outside the scope of the PayLINK. Applications must not interfere with the use of a two- factor authentication mechanism. If customers can use remote access software, then customers and resellers/integrators must implement a two-factor authentication mechanism (user ID and password plus an additional authentication item such as a smart card, token or PIN) for remote access to the application. Customers and reseller/integrators must be instructed to use and implement remote access software security features as described below:

- All users are assigned a unique ID for access to system components or cardholder data.
- Change default settings in the remote access software.
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins.
- Enable encrypted data transmission.
- Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13.
- Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

2.12. Encrypt Sensitive Traffic Over Public Networks

All traffic sent by PayLINK is sent via SSL (SSL, HTTPS, WS, and 2SSL are all based on SSL). Integrators should **NEVER** touch, store, collect or send cardholder data by end-user messaging technologies (for example, e-mail, instant messaging, and chat).

Applications integrating to PayLINK **do not have access** to cardholder data via the PayLINK interface. Additionally, these integrated applications should **NEVER** touch, collect or store the account holder's actual card information. Doing so will result in the POS application being non-compliant with PA-DSS.

The vendor's application Implementation Guide provided should contain guidance to the customer to never send unencrypted cardholder data by end-user messaging technologies (for example, e-mail, instant messaging, and chat).

2.13. Encrypt All Non-Console Administrative Access

This requirement is outside of the scope of PayLINK. If an application allows non-console administration, use SSH, VPN, or SSL/TLS for encryption of non-console administrative access.

2.14. Maintain Instructional Documentation and Training Programs for Customers

This requirement is outside the scope of the PayLINK. The vendor should develop and maintain documentation and training for their customers.

2.15. Additional Information

The Payment Application Data Security Standard (PA-DSS) is available from the PCI Security Standards Council Web site at: https://www.pcisecuritystandards.org/