Apple Pay In-App Provisioning Security
Entitlement Guidelines

Version 1.0
May 22, 2015

Confidentiality

The contents of this document, as well as any appendices, supplements, or follow up communications, are confidential and proprietary. They should be shared only with disclosed individuals, and on a need to know basis withIn-Apple, and with disclosed partners.

If you are not certain that you are disclosed, or that you should have access to this document, please stop reading now, and consult the appropriate legal resource within your company before proceeding.

Version Information

Date	Version	Changes
05/22/2015	Initial	

Target Audience

This guide will provide Apple Pay issuers with guidelines to ensure appropriate security precautions are in place to facilitate In-App provisioning for Apple Pay payment instruments.

Guidelines

Every App requesting the Apple Pay In-App Provisioning entitlement must implement controls designed to provide for secure card provisioning from inside the issuer's application. These controls are intended to further protect users from phishing and account takeover attempts.

Qualification

Qualification is verification during App review that the issuer app meets the minimum requirements to ensure the controls are in place to enable In-App provisioning. In-App provisioning can only be enabled through entitled Apps that are available through App Store. In-App provisioning functionality will not be available for any apps that have not received the entitlement.

Minimally Acceptable Criteria for Utilizing In-App Provisioning

In order to utilize in-app provisioning, an application must meet a) the Security Controls Requirements and b) Multi-Factor Authentication Requirements set forth below. An issuer must also be able to apply the additional security measures outlined for an Orange Path / Code 0G as set forth below. Exceptions to full compliance with the requirements below require written approval from Apple.

Security Controls Requirements

Qualification requires that an application meet all of the Security Controls Requirements set forth below:

Security Control	Definition
Strong Password Policy	Requiring a combination of at least two of the following: - uppercase letters (e.g. A, B, C) - lowercase letters (e.g. a, b,c) - numeric characters (e.g. 1, 2, 3) - special characters (e.g. $, ?, &)
Minimum Password Length	Requiring a minimum length for passwords greater than ~~seven~~ six characters
Maximum Attempts Policy	Locking the user account after a specified maximum number of attempts
Updated Credentials Controls	Requiring use of different tenured channels or call center verification if the application user credentials (i.e., username and/or password) have been changed within a defined window (e.g., 60 days) prior to the provisioning attempt

Multi-factor Authentication

All provisioning from in-app requires that multi-factor authentication of the user has been applied at least once prior to the activation of the provisioning attempt. There are two approved approaches to implement Multi-factor Authentication:

i) Unrecognized Device Multi-factor Authentication

Multi-factor authentication utilizing a one-time password ("OTP") communicated to a tenured channel ("MFA") should be applied for new and unrecognized devices to ensure that the user is verified during the first attempt to access a newly installed app. If the same app on the same device is subsequently used to provision a card into Apple Pay, the original MFA satisfies the MFA requirement for in-app provisioning.

ii) In-App Provisioning with a One Time Passcode

If an issuer does not do an MFA at the time of app installation, an MFA must be done at the time of provisioning to validate the user identity of the person seeking to provision the card. This can be done utilizing the standard Yellow Flow capabilities of the platform (one-time password through a tenured channel, or if none is available, via a call to the call center; note, in-app verification may not be used in lieu of SMS, email or call center when the result would be to use in-app verification to verify the app (as no additional security would be provided)).

Use of Apple Provisioning Data - In-App Provisioning and Orange Flow (Code 0G)

In addition to the Security Controls Requirements and the Multi-Factor Authentication Requirements, an issuer should be able to meet the minimum requirements for Orange Path/Code 0G set forth below.

As context, Apple has implemented a Reason Code 0G (also known as "Orange Path") as part of the data shared by Apple with issuers for use during the provisioning process. Where Apple indicates Orange Path / Code 0G in connection with a specific provisioning attempt, Apple is indicating to the issuer the existence of factors suggesting that the issuer should exercise a high degree of diligence before approving the specific provisioning request.

In the context of In-App Provisioning, Apple requires that any In-App Provisioning attempt for which Apple responds with Orange path / Code 0G be subject to additional authentication rigor. Specifically, for any such attempt, the issuer is expected to do an updated OTP step to a tenured channel (in the case of a dated OTP) or require a call into a call center if no additional tenured channel is available. We also recommend steps like adding a requirement of entry of the CVV from the card as part of the issuer's user interface within their application. Note: issuers may choose to deploy multiple of these practices with an Orange Path provisioning effort (and issuers are permitted to use any of these practices or other security practices within their UI as they deem appropriate, including in the absence of Orange Path/Code 0G indicators from Apple). In this context, best practice will be to design for flexibility in enabling a range of additional verification measures when either the issuer's systems indicate an "orange / red flow" or where Apple's data indicates elevated risk.

Note: It is highly recommended that issuers have additional verification steps ready and available for inclusion in their In-App Provisioning flow within their banking application. For example, many banks deploy a one-time SMS to a verified channel for every meaningful change to an account set-up (e.g., adding a new payee into online bill payment, changing contact information) as well as sending email notifications of such changes concurrently to the tenured email address. Ability to gather CVV or ask additional "out-of-wallet" security questions may also be a useful verification step. Addi-

tion of these capabilities, even if only used selectively, give issuers significant risk mitigation capabilities.

Provisioning Notifications

Notifications of successful provisioning (i.e., activation) are required to ensure the user is aware that their card was successfully added to Apple Pay. This can be accomplished by sending an electronic communication (e.g., email) or paper letter to a tenured address of record.

Revocation of Privileges

In order to ensure that users are protected from fraudulent provisioning, Apple reserves the right to disable In-App Provisioning through all of the following methods, including, but not limited to:

- Sending provisions through Yellow flow requiring One Time Passcode for all In-App provisioning requests
- Blocking In-App provisioning for specific versions of the App
- Blocking In-App provisioning at the issuer level
- Disabling the App altogether

Issuer Certification

As part of the application submission and review process for apps that seek to incorporate In-App Provisioning, Apple will request a bank certification as to compliance with the elements of this guidelines document. Apple reserves the right to request demo accounts (login / password) in order to validate elements of the functionality described herein.