jack henry™

Jack Henry Digital Provisioning Enablement™ Product Guide

Table of Contents

Introduction

The purpose of this document is to assist Jack Henry clients along with their digital banking providers in understanding integration dependencies and steps to support digital provisioning and digital issuance. Non-Jack Henry core client integration dependencies and requirements may differ and require further evaluation by the affected financial institution (FI).

Digital Provisioning Overview

Digital provisioning is the process of securely pushing the card information from a digital banking application to a digital wallet (ex: Apple Pay®, Google Pay™, Samsung Pay™). This can be done using in-app provisioning (app to app) or web push provisioning.

Why?

Digital provisioning streamlines the process of adding an activated card to a digital wallet. While your cardholders can continue to manually add card/account details to a digital wallet, digital provisioning removes this requirement.

More importantly, digital provisioning enables non-activated cards (cards ordered, but not yet received or activated by the cardholder) to be provisioned to a digital wallet. Once provisioned, the cardholder can use the digital wallet for transactions in store and online while waiting for their physical plastic to arrive. Without digital provisioning, cardholders are not able to add a card to a digital wallet until the physical plastic is received and activated.

Use Cases

New Account

Ability to request new account/card for immediate use.

1. User applies for a new account.
2. Account is created on the core (debit/IHC) and/or switch (FSC).
3. Cardholder can view account in digital banking and select the option to push their card to the digital wallet.
4. Cardholder can use digital wallet in store and online.

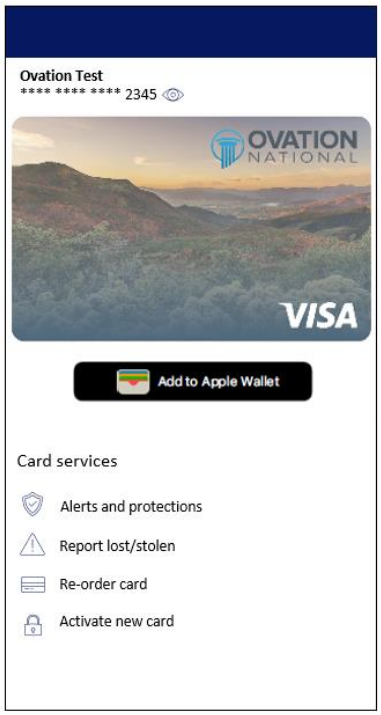
Lost/Stolen Card Replacement

Ability to report existing card lost/stolen and request a new card for immediate use.

1. Cardholder reports their card lost/stolen and requests a new card.

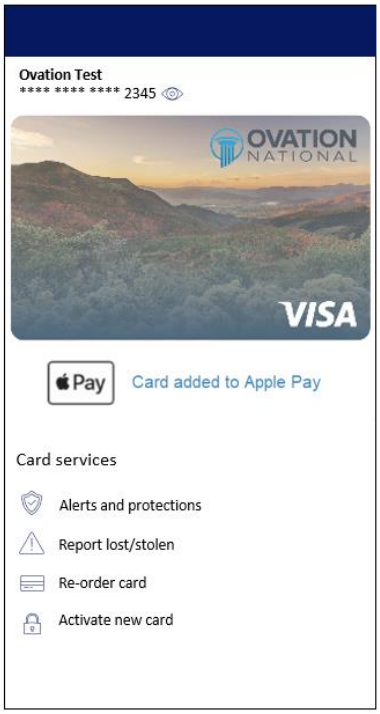
2. Card is flagged as lost/stolen on the core (debit/IHC) and/or switch (FSC) and a replacement card request is generated.
3. Core/switch creates new card number.
4. Cardholder can view new card in digital banking and select the option to push their card to the digital wallet.
5. Cardholder can use digital wallet in store and online.

High-Level Process (In-App Provisioning)



1. Cardholder sees their issued card within their FI's mobile banking app where they can select the provisioning option (add to Apple Wallet in example above).*

2. Cardholder is sent to the wallet interface to agree to the FI's terms and conditions for provisioning.



3. Once agreed upon, the card is added to the Pay wallet and the cardholder is returned to the FI's app.

*In the back end, the mobile banking application determines if the *Add to Wallet* button will be displayed. Some of the considerations are card status (including activation), if the card is already in the wallet, and if the FI supports loading non-activated cards.

NOTE: The images above are for demonstration only and do not reflect actual design.

High-Level Process (Web Push Provisioning)

1. The cardholder logs into their FI's digital banking platform and selects the option to provision their issued card to a digital wallet.
2. Upon selection, the cardholder is prompted to authenticate with their chosen digital wallet provider (e.g., Apple, Google)
3. A list of the cardholder's eligible devices associated with the wallet provider is displayed. The cardholder selects the device where they want the card provisioned
4. The cardholder reviews and accepts the terms and conditions for adding their card to the digital wallet.
5. The card is added to the selected digital wallet and is ready for use.

Considerations

PIN Selection

Cardholders need to be able to select a PIN for a digitally provisioned card. The recommended approach is to offer PIN selection in digital banking. Digital banking vendors may choose to integrate with an instant issue or fintech vendor to offer PIN selection. In this scenario digital banking partners with the instant issue or fintech vendor to provide the necessary inputs so that the vendor can create the PIN offset (the FI may not necessarily need to have a direct relationship with the instant issue vendor). Functionality and vendor support is evolving. This document will be updated as more is learned.

Depending on your FI's PIN selection settings, an update may be required to allow PIN selection via IVR before the cardholder receives and/or activates their card.

- JHA Card Activation and PIN Management™ requires the card be activated to set a PIN. If the card is not activated, the cardholder will be prompted to activate before they are prompted to set a PIN.
    - To support IVR PIN selection without activation, **JHA Digital PIN Management** needs to be implemented. ***NOTE: This IVR has a different phone number than JHA Card Activation & PIN Management. FIs that do not display card credentials will need to provide the PAN to cardholders that want to select a PIN before receiving their physical card.***
- JHA PIN Management™ service (without card activation) typically uses CVV2/CVC2 as a required token. If CVV2/CVC2 is required and your FI is not displaying card credentials in digital banking, a change will be needed to your required tokens to allow PIN selection before the plastic is received. Also, FIs that do not display card credentials will need to provide the PAN to cardholders that want to select a PIN before receiving their physical card.

NOTE: FIs using First PIN as an activation element on the core, could have cards activated before they are received if a cardholder performs a PIN transaction using their digital wallet.

Using MyCardRules™

If using MyCardRules integrated with digital banking, your digital banking vendor will control if a new card is added while pending activation or if it is only added after the card is activated.

If using the Jack Henry stand-alone application, the card number, CVV2/CVC2, and expiration date are needed before a new card can be added to MyCardRules. If you are displaying card credentials in digital banking, the cardholder will be able to add their new card to MyCardRules before it is activated.

Digital Issuance Overview

Digital issuance, also referred to as digital first, enables card credentials to be issued in digital banking while waiting for a new card to arrive or when suppressing physical card production. It leverages a combination of digital provisioning and the ability to view card details. The FI is responsible for deploying strong cardholder authentication in the digital environment for viewing card credentials. ***NOTE: Supporting digital issuance while waiting for a new card to arrive requires digital provisioning of cards that have not been activated and temporary expiration date support.*** If suppressing physical card production, see the Digital Only section below for additional information.

Why?

Digital issuance enables non-activated cards (cards ordered, but not yet received or activated by the cardholder) to be provisioned to a digital wallet. Once provisioned, the cardholder can use the digital wallet for transactions in store and online while waiting for their physical plastic to arrive. Additionally, digital issuance allows a cardholder to view card credentials so they can shop online (where a digital wallet is not supported) prior to receiving and activating the plastic card. This enables the cardholder to transact digitally across available channels soon after the card is issued.

Use Cases

New Account

Ability to request new account/card for immediate use.

1. User applies for a new account.
2. Account is created on the core (debit/IHC) and/or switch (FSC).
3. Cardholder can view account in digital banking and select the option to push their card to the digital wallet.
4. Cardholder can use digital wallet in store and online.
5. Cardholder authenticates to view card credentials within the digital platform.
6. Cardholder can use card credentials for online shopping.

Lost/Stolen Card Replacement

Ability to report existing card lost/stolen and request a new card for immediate use.

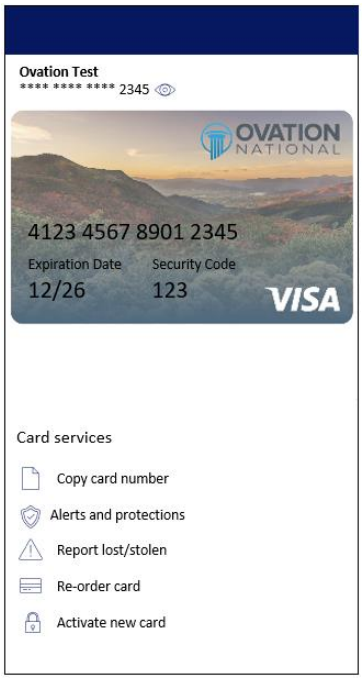
1. Cardholder reports their card lost/stolen and requests a new card.
2. Card is flagged as lost/stolen on the core (debit/IHC) and/or switch (FSC) and a replacement card request is generated.
3. Core/switch creates new card number.
4. Cardholder can view new card in digital banking and select the option to push their card to the digital wallet.
5. Cardholder can use digital wallet in store and online.
6. Cardholder authenticates to view card credentials within the digital platform.
7. Cardholder can use card credentials for online shopping.

High-Level Process

See the high-level process for provisioning in the digital provisioning section.

1. Cardholder sees their issued card within their digital platform and selects option to view card details.

2. Cardholder is authenticated using strong authentication*.



3. Full card number, expiration date and CVV2/CVC2 are shown. Option to copy card number provided.

*In the back end, the digital platform obtains a useable expiration date and initiates a jXchange call to obtain the CVV2/CVC2.

NOTE: The images above are for demonstration only and do not reflect actual design.

Digital Only Overview

Why?

As contactless acceptance continues to grow, certain cardholders may prefer a digital only card and not a physical plastic. When a digital only card is preferred by the cardholder, a physical plastic will not need to be issued. This reduces FI expenses for cardholders that do not plan to use a physical plastic.

Some FIs may choose to issue two separate card numbers to a consumer (a digital only card and a physical card). Since the digital only card is issued active, this approach may remove the complexities of handling authorizations on non-activated cards. Additionally, the digital only card number will not need to change if the physical plastic is lost/stolen. However, it may introduce other complexities since the digital banking vendor will need to differentiate between the digital only and physical card and be able to control which can be provisioned to a digital wallet and displayed when viewing card credentials. Also, this approach may cause cardholder confusion when the card details are printed on the physical plastic as the physical card and digital only credentials will not match.

Use Cases

New Account

Ability to request new account with a digital only card.

1. User applies for a new account.
2. User requests a digital only card (no plastic).
3. Account is created on the core (debit/IHC) and/or switch (FSC) and the card is in an activated state.
4. Cardholder can view account in digital banking and select the option to push their card to the digital wallet.
5. Cardholder can use digital wallet in store and online.
6. Cardholder authenticates to view card credentials within the digital platform.
7. Cardholder can use card credentials for online shopping.

Lost/Stolen

Ability to report existing card lost/stolen and request a new card for immediate use.

1. Cardholder reports their card lost/stolen and requests a new digital only card.

2. Card is flagged as lost/stolen on the core (debit/IHC) and/or switch (FSC) and a replacement card request is generated.
3. Core/switch creates new card number.
4. Cardholder can view new card in digital banking and select the option to push their card to the digital wallet.
5. Cardholder can use digital wallet in store and online.
6. Cardholder authenticates to view card credentials within the digital platform.
7. Cardholder can use card credentials for online shopping.

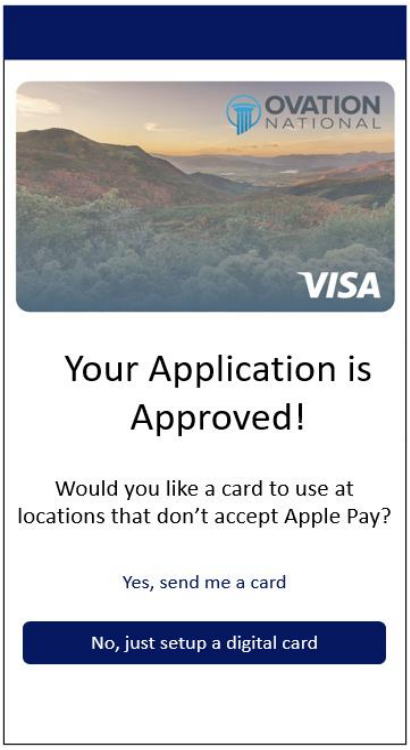
Request Physical Card for Digital Only Account

1. Cardholder requests a physical plastic be added to their digital only account.
2. Digital platform sends call to the core (debit/IHC) or switch (FSC) to request a physical plastic be added to the account.
3. A plastic is created for the already issued card number.
4. Cardholder can continue to view card credentials within the digital platform for use with eCommerce merchants.

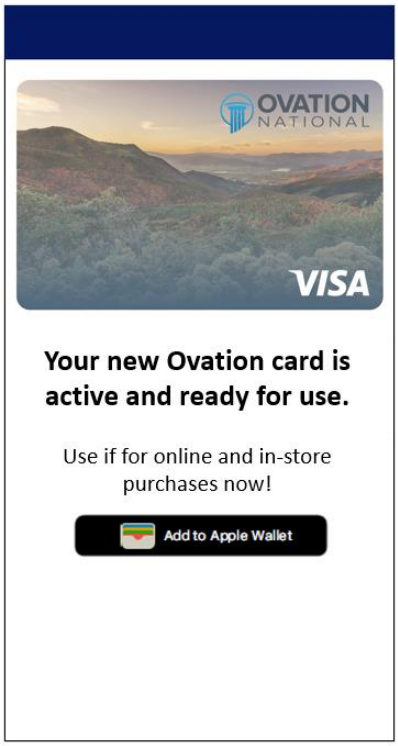
Potential Alternate Workflow (if supported by FI, core, and digital platform): Request Both Physical Card and Digital Only Card on New Account

1. User applies for a new account/card.
2. Digital platform integration with the core (debit/IHC) or switch (FSC) to create account and request both a physical card (Silverlake, CIF 20/20: card category EMV or DIC) and digital only card (Silverlake, CIF 20/20: card category DGT) with different card numbers.
3. Issuance of cards/account upon decisioning in near-real time after application.
4. Digital platform differentiates between physical card (Silverlake, CIF 20/20: card category EMV or DIC) and digital only card (Silverlake, CIF 20/20: card category DGT) to offer push provisioning and view card credentials on digital only card.
5. Cardholder initiates push provision of digital only card credentials directly into digital wallets.
6. Cardholder authenticates to view card credentials within the digital platform for use with eCommerce merchants. Digital only card credentials are displayed.

High-Level Process



1. Cardholder applies for or requests new digital only card.



2. Cardholder notified their new card is active and given the option to provision it to the digital wallet.

NOTE: The images above are for demonstration only and do not reflect actual design.

See the high-level process for provisioning in the digital provisioning section and for displaying card credentials in the digital issuance section.

Availability Charts

Digital Provisioning and Digital Issuance

	Digital Provisioning and Displaying Card Details	JH Core System*	Digital Banking	CPS Switch	jXchange**
Debit and IH Credit	activated card	Available	Check with provider for integration status	Available	Available
	non-activated card	SilverLake-CIF 20/20: R2023 Core Director: R2026 for CPS FIs only Symitar: Release 2021.01	Check with provider for integration status	Available	Available
FS Credit	activated card	Symitar: Available CIF 20/20, Core Director, SilverLake: Clear PAN solution timing TBD	Check with provider for integration status	Available	Available
	non-activated card	Symitar: Available CIF 20/20, Core Director, SilverLake: Clear PAN solution timing TBD	Check with provider for integration status	Available	Available

*Non-Jack Henry core requires FI evaluation.

**Symitar clients obtain card data from SymXchange™ and CVVs/CVC2 from jXchange.

Digital Only Issuance

	Digital Only Issuance	JH Core System*	Digital Banking	CPS Switch	jXchange
Debit and IH Credit	activated, plastic card suppressed	SilverLake-CIF 20/20: R2023 Core Director: R2026 for CPS FIs only Symitar: CWR needed to scope/implement changes	Check with provider for integration status	Available	Available
FS Credit	activated, plastic card suppressed	Symitar: Available CIF 20/20, Core Director, SilverLake: Clear PAN solution timing TBD	Check with provider for integration status	Available	Available

*Non-Jack Henry core requires FI evaluation.

Digital Provisioning Technical Details

Pre-requisites and integration requirements must be met before digitally provisioning cards. ***NOTE: The digital provisioning process needs to account for the card activation status. Financial institutions should***

only provision cards that are active unless all functionality to support non-activated cards has been implemented on the core and /or transaction processing switch (aka JHA Debit Processing™ or JHA Credit Processing™).

Prerequisites

- FI must be setup for tokenization with digital wallets they want to provision.
- Digital banking provider integrates with each digital wallet they want to support or an available software development kit (SDK).
- Digital banking provider integrates with the core for debit and in-house credit (IHC) or the switch for full-service credit (FSC) to obtain card information, including card activation status and if the FI allows provisioning issued, not activated cards. ***NOTE: Some cores require digital banking provider update the core when a card is digitally issued.***
- The account must be on the switch at time of provisioning. Cards added via batch file vs an online maintenance message or instant issue can only be provisioned following nightly processing.
- FI must initiate a project with Jack Henry for Provision Plus (see Provision Plus section for more information) before provisioning non-activated cards.
- FI must have a mechanism for the cardholder to select a PIN when a card is pending activation.

Integration Requirements

Provisioning non-activated cards may require core changes. The core must support authorization of token transactions on non-activated cards, as noted below, before these cards can be provisioned in digital banking. The switch currently supports token transactions on non-activated cards.

CIF 20/20 and SilverLake (debit)

Provisioning non-activated cards requires core changes.

- FI must be on Release 2023 or later and ISO level flag Allow Digital/Inactive Provision (Y/N) must equal Y.
    - If the Allow Digital/Inactive Provision (Y/N) indicator is not Y and a non-activated card is provisioned, digital wallet authorizations will be declined until the card is activated.
    - If Allow Digital/Inactive Provision (Y/N) indicator is Y, authorizations with a token will be approved while the card is not activated.
- The setting identifying if the ISO allows digital provisioning on non-activated cards can be retrieved by the digital banking provider in one of two calls:
    - ParmValSrch for EFTCardProdCode will contain the ISO setting in element *Allow Digital InActive Type <AllowDigitalInActType>*.
    - EFTCardInq will contain the ISO setting in element *Allow Digital InActive Type <AllowDigitalInActType>*.

- jXchange call EFTCardInq provides the card activation status in field *<EFTCardStatType>*. The following values represent cards that have been issued but not activated.
    - InstantIssMail
    - OrderCard
    - OrderInProc
    - ReOrderCard

Core Director (CPS processed debit)

Core Director supports provisioning non-activated cards for CPS FIs with Release 2026.

- FI must be on Release 2026 or later and ISO level flag in program ATMPSO for "Approve Provisioned Transactions" (Y/N) must equal Y.
    - If the Approve Provisioned Transactions (Y/N) indicator is N and a non-activated card is provisioned, digital wallet authorizations will be declined until the card is activated.
    - If Approve Provisioned Transactions (Y/N) indicator is Y, authorizations with a token will be approved while the card is not activated.
- The setting that determines whether a ISO supports digital provisioning on non-activated cards can be retrieved by the digital banking provider in one of two API calls:
    - ParmValSrch for EFTCardISOCode with the values below:

      <ParmName>**EFTCardISOCode**</ParmName>
      <ParmSvcName>**EFTCard**</ParmSvcName>

      ISO details will be returned as follows:

      <ParmValSrchRec>
       <ParmValCode>**555555**</ParmValCode>
       <ParmValDesc>**Visa Card**</ParmValDesc>
       <ParmValInfoArray>
        <ParmValInfo>
         <ParmValDetail>**true**</ParmValDetail>
         <ParmValTxt>**AllowDigitalInActType**</ParmValTxt>
        </ParmValInfo>
       </ParmValInfoArray>
      </ParmValSrchRec>
    - EFTCardInq will contain the ISO setting in element *Allow Digital InActive Type <AllowDigitalInActType>*.
- jXchange call EFTCardInq provides the card activation status in field *<EFTCardStatType>*. The following values represent cards that have been issued but not activated.
    - OrderCard
    - OrderInProc

- ReOrderCard

Symitar (debit and IHC)

Provisioning non-activated cards requires core changes.

- FI must be on Release 2021.01 or greater.
- When a card is created in Symitar, the expiration date needs to be set at the time of creation. This can be configured within Card Creation Wizard parameters.
- When digital banking provider digitally provisions a card that has already been issued (card status field is set to issued and the Issue Date field is populated) on Symitar, they need to set the field *Digital Issue Status* to *6*. This means the digital issue is complete. ***NOTE: If the card status field is set to issued and the Digital Issue Status is already set to 4, it should NOT be changed to 6.***
- When digital banking provider provisions a card in pending card order status (Not Issued) or digital banking provider requests a card order and the card will be digitally provisioned, the following fields need to be updated on Symitar.
  - *Digital Issue Status* = *4* (Digital Issue Success - Pending Plastic)
  - *Card Status* = *1* (Issued)
  - *Effective Date* = Current date
  - Digital banking provider also needs to validate that the expiration date has been set.
- If *Digital Issue Status* is not set, digital wallet authorizations will be declined until the card is activated.
- If *Digital Issue Status* is set, the Symitar system will ignore the card activation status and expiration date checking when processing authorizations, regardless of the presentation instrument (digital wallet/token transaction or physical plastic). Once the physical card is activated and the card activation date is populated, then card activation and expiration date checking will be in place if set to do so in parameters. ***NOTE: If FI uses card activation on the processing platform, Jack Henry will only allow token transactions to flow to Symitar when the card is not activated.***

Full-Service Credit

All cards can be provisioned regardless of activation status. Digital banking provider needs unencrypted PAN to provision.

- CIF 20/20, Core Director, SilverLake: Clear PAN solution timing TBD.
- Symitar: Available

Non-Jack Henry core

- FIs should contact their core to determine if digital banking provider is required to look at certain fields to determine if non-activated cards can be provisioned or if digital banking provider needs to set any flags when provisioning a card.

- FIs should contact their core to determine if updates are required to authorize token transactions on non-activated cards.
- If the core does not have the card activation status, the digital banking vendor is required to integrate with jXchange call CrCardHolderInq to determine if the card has been activated on the switch. If the *<CrCardActDt>* field contains a value of 0001-01-01 the card has not been activated. If activated, it will contain the activation date. A project with Jack Henry to enable the jXchange call may be required.

Provision Plus (Visa and Mastercard only)

Provision Plus is a rules engine used in conjunction with the processing platform to determine if token provisioning requests should be approved, declined, or require additional authentication. ***Provision Plus is required before provisioning a card that has not been activated.*** This product allows push provisioning requests to be approved regardless of the activation status. Without this product, provisioning requests on cards pending activation will be declined.

In addition to supporting provisioning while the card is pending activation, Provision Plus will be used to bypass yellow status (additional authentication) for green (approval) when digitally provisioning. This is done using the PAN Source value supplied by the card brand.

A contract addendum and project with Jack Henry is required to implement Provision Plus. Once Provision Plus is implemented, **all** token provisioning requests will route through this product, not just push provisioning requests. Token provisioning requests include:

- Digital wallet: Cards added to wallets such as Apple Pay, Google Pay, etc. whether manually entered or push provisioned.
- Device binding: Enables COF, e-commerce enabler, and web browser tokens provisioned to the consumer's account to be bound to multiple trusted devices.
- Card/credential on file: Cards stored on file with merchants and online checkout solutions such as Click to Pay, PayPal, BNPL lenders, etc. that support tokenization.

You can estimate costs by reviewing the CD-3807, summary line TA – Token Acct Validation. After implementing Provision Plus, the billing counts will be on summary line TD – Token Provision Decision.

Digital Issuance Technical Details

Pre-requisites and integration requirements must be met before offering digital issuance functionality.

Prerequisites

- Must support prerequisites and integration requirements in *Digital Provisioning Technical Details* section.
- Digital banking provider integrates with the core and/or the switch for to obtain card information, including card activation status and expiration dates, and set the temporary expiration date (when required).
- Digital banking provider integrates with jXchange to obtain the CVV2/CVC2.
- The account must be on the switch at time of provisioning. Cards added via batch file vs an online maintenance message or instant issue will not be able to view card credentials until after nightly processing.
- FI may need to initiate a project with Jack Henry to enable jXchange calls.
- FI must have a mechanism for the cardholder to select a PIN when a card is pending activation.

Integration Requirements

Before card credentials can be displayed in digital banking, the core must be able to authorize card not present/eCommerce purchases that contain a temporary expiration date when the physical plastic is not activated and there is not a valid previous expiration date. The switch currently supports transactions with a temporary expiration date.

If the card is activated, the current expiration date is used when obtaining the CVV2/CVC2 and displaying card credentials.

If the card is not activated, the following information should be used to determine which expiration date should be used when obtaining the CVV2/CVC2 and displaying card credentials:

- If there is a valid previous expiration date this date is used.
- If there is not a valid previous expiration date but there is a valid temporary expiration date (CIF 20/20 and SilverLake) this date is used.
- If there is not a valid previous or temporary expiration date, digital banking application makes API calls to set a temporary expiration date on the switch and core (depending on core functionality). The new temporary expiration date is used when obtaining the CVV2/CVC2 and displaying card credentials.

jXchange (all FIs)

Digital banking provider integrates with two jXchange calls.

- CardCVVInq to obtain CVV2/CVC2.
    - Element CardVerifId provides the CVV2/CVC2 value. This is a numeric field, so the leading zeros may not appear. Before displaying the value to the cardholder, add leading zeros so the value displayed is a three-digit value.
    - Element CardCVVId provides the CVV2/CVC2 value as a string.
- Must use an expiration date that is activated in the CVV2/CVC2 call. If the card is issued but not activated and there is not a valid temporary or previous expiration date, jXchange call CardTempExpDtMod must be used to set a temporary expiration date on the switch. This temporary expiration date should be set to the end of the following month, and it needs to be used in the CardCVVInq call. ***NOTE: If the current expiration date is not yet activated and there is a valid previous expiration date, the previous expiration date should be used in the CardCVVInq call. If a temporary expiration date is set instead, the card bearing the previous expiration date will stop working.***

CIF 20/20 and SilverLake (debit)

Displaying card credentials using a temporary expiration date requires core changes. Before setting a temporary expiration date, digital banking provider must make sure the core is ready for this functionality.

- FI must be on Release 2023.
- After successfully setting a temporary expiration date on the switch through CardTempExpDtMod, it must also be set on the core using EFTCardMod, element *EFT Card Temporary Expiration Date <EFTCardTempExpDt>*.
- Token or card not present/eCommerce transactions will be authorized if the temporary expiration date is set on the switch and core and used in the purchase.

Core Director (CPS processed debit)

Core Director supports displaying card credentials for non-activated cards for CPS FIs with Release 2026.

- FI must be on Release 2026.
- After successfully setting a temporary expiration date on the switch through CardTempExpDtMod, it must also be set on the core using EFTCardMod, element *<EFTCardAltExpDt>*. This will populate the temporary expiration date in the Credential Expiration Date on Core Director.
- Token or card not present/eCommerce transactions will be authorized if the temporary expiration date is set on the switch, the credential expiration date is set on the core and used in the purchase.

Symitar (debit and IHC)

- After successfully setting a temporary expiration date on the switch through CardTempExpDtMod, it must also be set on the core via SymXchange™. The temporary expiration date will need to be loaded into the *Previous Expiration Date* field in the Card Record.
- The *Digital Issue Status* must also be set to *4* or *6* (as applicable) and the card status must be issued. **See the Symitar section under the Digital Provisioning Technical Details for details.**
- Transactions will be authorized if the digital issue status is set, and the temporary expiration date is set on the switch and core and used in the purchase.
- If *Digital Issue Status* is set, the Symitar system will ignore the card activation status and expiration date checking when processing authorizations, regardless of the presentation instrument (digital wallet/token transaction or physical plastic). Once the physical card is activated and the card activation date is populated, then card activation and expiration date checking will be in place if set to do so in parameters. ***NOTE: If FI uses card activation status and expiration date mismatch on the processing platform, Jack Henry will only allow expected transactions to flow to Symitar when the card is not activated.***

Full-Service Credit

- Must use call CrCardHolderInq to obtain previous expiration *<CrCardPrevExpDt>* (if current expiration is not activated). If a valid expiration date is not returned in this field, a temporary expiration date must be set.
- Digital banking provider needs unencrypted PAN.
    - CIF 20/20, Core Director, SilverLake: Clear PAN solution timing TBD.
    - Symitar: Available
- Transactions will be authorized if the temporary expiration date is set on the switch and used in the purchase.

Non-Jack Henry core

- If the core does not have the card activation status, the digital banking vendor needs to integrate with jXchange call CrCardHolderInq to determine if the card has been activated on the switch. If the *<CrCardActDt>* field contains a value of 0001-01-01 the card has not been activated. If activated, it will contain the activation date. A project with Jack Henry may be required to enable the jXchange call.
- FIs whose core does not store the previous expiration date can use call CrCardHolderInq to obtain previous expiration *<CrCardPrevExpDt>* (if current expiration is not activated).
- FIs whose core stores the previous expiration date need to allow digital banking providers to update this date with a temporary expiration date or they need to support a temporary expiration date field.

- FIs should contact their core to determine if the digital banking provider needs to look at certain fields to determine if a temporary expiration can be used and if updates need to be made to authorize card not present/eCommerce purchases with a temporary expiration date.

Visual Details

All the prerequisites listed above must be met before displaying card details for non-activated cards.

- Digital banking application must reauthenticate the user before showing card details. Biometric authentication is the best method; however, passcode or OTP can also be used.
- Digital banking vendor must follow card brand standards when displaying card art and credentials. ***NOTE: To ensure card brand requirements are met when displaying card art, the digital banking vendor should use the same card art that was approved for use in the digital wallet.***
    - Mastercard customers should reference the Mastercard *Card Design Standards*, Non-Tokenized Card Image Standards section for full requirements when displaying card art or credentials.
    - Visa does not have standards related to displaying card credentials.
- Displaying the following details is recommended:
    - Digital card art.
    - Full primary account number (PAN).
    - PAN expiration date that was sent in jXchange call CardCVVInq. ***Must use an expiration date that is activated.***
    - CVV2/CVC2 security code obtained through jXchange call CardCVVInq.
    - Ability to copy card number.
    - ***NOTE: If a cardholder adds card credentials with a temporary or previous expiration date to subscription services or recurring payments and the merchant doesn't support account updater services, the cardholder will need to update their credentials with the merchant when the temporary or previous expiration date expires or is replaced.***
        - Digital banking providers may want to consider a warning or pop-up message to address this scenario.

Digital Only Technical Details

Pre-requisites and integration requirements must be met before offering digital only functionality.

Prerequisites

- Core/switch must support digital only cards.
- FI must have a mechanism for the cardholder to select a PIN.
- Digital banking:

  - Must support digital provisioning.
  - Must have the ability to display card details.
  - Ability to send push notification when card is issued or reissued (recommended).
- The account must be on the switch at time of provisioning. Cards added via batch file vs an online maintenance message or instant issue will not be able to view card credentials until after nightly processing.

Integration Requirements

Digital only may require core changes. The core must support generating an activated card number and expiration date without issuing a plastic. They must be able to authorize token and eCommerce/card not present transactions on digital only cards. When generating reissues, the core must be able to extend the expiration date of digital only cards without issuing a plastic.

CIF 20/20 and SilverLake (debit)

- FI must be on Release 2023 or later.
- ISO flag *Allow Digital Only Cards (Y/N)* must be *Y*.
- The setting identifying if the ISO allows digital only cards can be retrieved by the digital banking provider in one of two calls:
  - ParmValSrch for EFTCardProdCode contains the ISO setting in element *Allow Digital Only Type <AllowDigitalOnlyType>*.
  - EFTCardInq contains the ISO setting in element *Allow Digital Only Type <AllowDigitalOnlyType>*.
- jXchange call EFTCardInq contains element *EFT Card Category <EFTCardCat>*, value *DGT*, to identify if the card is digital only.
- To issue a digital only card, the *EFT Card Category <EFTCardCat>* element in the new account message should be set to *DGT*. This element is included in jXchange calls EFTCardAdd and EFTCardMod.
- A physical plastic is not issued, and card is set as activated.
- Authorization is restricted to transactions with a token or card not present/eCommerce.
- When a new digital only card is issued due to expiration reissue, both digital only cards will work until the old one expires.
- When a new digital only card is issued due to compromise, the old digital only card will stop working with the first transaction on the new digital only card.
- *If* the FI wants to allow cardholders to later request a physical plastic, the EFTCardMod call can be used. The *EFT Card Category <EFTCardCat>* element should be set to the FI's default value.
  - jXchange call ParmValSrch for EFTCardProdCode will contain the *ISO Default Card Category*. If this field is not *DGT*, the value in this field can be used to request a plastic.

- If the *ISO Default Card Category* is *DGT* and there is a value in the *Alternate Card Category* field, it can be used to request a plastic.

Core Director (CPS processed debit)

Core Director supports digital only for CPS FIs with Release 2026.

- FI must be on Release 2026 or later.
- ISO level flag *Allow Digital Only (Y/N)* must be *Y*.
- The setting that determines whether a ISO allows digital only cards can be retrieved by the digital banking provider in one of two calls:
  - ParmValSrch for EFTCardISOCode with the values below:

    <ParmName>**EFTCardISOCode**</ParmName>

    <ParmSvcName>**EFTCard**</ParmSvcName>

    ISO details will be returned as follows:

    <ParmValSrchRec>
    <ParmValCode>**555555**</ParmValCode>
    <ParmValDesc>**Visa Card**</ParmValDesc>
    <ParmValInfoArray>
    <ParmValInfo>
    <ParmValDetail>**true**</ParmValDetail>
    <ParmValTxt>**DigitalOnly**</ParmValTxt>
    </ParmValInfo>
    </ParmValInfoArray>
    </ParmValSrchRec>
  - EFTCardInq contains the ISO setting in element *Allow Digital Only Type <AllowDigitalOnlyType>*.
- jXchange call EFTCardInq contains element *EFT Card Category <EFTCardCat>*, value *DGT*, to identify if the card is digital only.
- To issue a digital only card, the *EFT Card Category <EFTCardCat>* element in the new account message should be set to *DGT*. This element is included in jXchange calls EFTCardAdd and EFTCardMod.
- A physical plastic is not issued, and the card is set as activated.
- Authorization is restricted to transactions with a token or card not present/eCommerce.
- When a new digital only card is issued due to expiration reissue, both digital only cards will work until the old one expires.
- When a new digital only card is issued due to compromise, the old digital only card will stop working with the first transaction on the new digital only card.

- Core Director does not support updating a digital only account to include a plastic card. *If* the FI wants to allow cardholders to later request a physical plastic, a separate account record will need to be created.

Symitar (debit and IHC)

FIs should open a CWR with Symitar to scope and implement necessary changes to their program.

FSC

FIs can setup an account without ordering a plastic by setting the plastic count to zero. Authorizations will be supported unless they are specific to a physical plastic. Upon renewal, the expiration date will be extended, and a plastic will not be issued unless the plastic count is greater than zero.

Non-Jack Henry core

FIs should contact their core to determine if digital only cards are supported and identify any related requirements for their digital banking provider.

Jack Henry Digital Provisioning Enablement Project

FI must be live with digital wallets before a digital provisioning enablement project will be started. A project with Jack Henry includes the following:

- Enablement of Provision Plus (**Visa and Mastercard only**).
    - Allow push provision to be approved when card is not activated.
    - Bypass yellow path for green path when digitally provisioned.
- Enablement of jXchange APIs used for displaying card details (if supported by digital banking provider). If your digital banking provider is not ready to support the APIs when Provision Plus is implemented, a separate project may be required when you are ready to add the APIs.

A separate project is needed to implement JHA Digital PIN Management or change the required tokens for JHA PIN Management.

Contact your CPS Customer Relationship Manager to initiate a project.