Apple Pay and Card Tokenization

FAQ

Be There. Be More.

CO-OP FINANCIAL SERVICES

Contents

FAQ

Apple Pay and Card Tokenization 3

Current Positions Of The Three Key Industry Players 3

Apple Pay Enrollment 4

Apple Pay Details 4

Apple Watch Payment Enablement 5

Tokenization Basics 7

Tokenization Details 8

Call Center 8

Transactions 9

Compliance 10

Consumers and Costs 10

Market 11

Apple Pay and Card Tokenization – What Are They?

What is Apple Pay?

Apple Pay™ allows you to pay for your purchases with your iPhone® 6, iPhone 6 Plus, iPhone 6s and iPhone 6s Plus and Apple Watch by holding your device near a contactless reader at participating merchants. You can also use your iPhone, iPad Air™, iPad Air™ 2, iPad Pro and iPad Mini™ 3 and 4 to pay within certain apps.

What is card tokenization?

Card tokenization is the process of replacing the traditional card account number (PAN) with a unique digital token in online and mobile transactions. Tokens can be restricted for transactions with a specific mobile device, merchant or transaction type. The tokenization process happens in the background in a way that is invisible to the consumer.

A payment token is a numeric substitute for a primary PAN and can be processed by all participants in the payments ecosystem. Payment tokens map back to the original PAN, providing the account issuer with the full transaction details.

Current Positions of the Three Key Industry Players

What's the latest on CO-OP Financial Services?

We are enrolling our credit unions that process signature debit or credit with us directly into Visa® and Mastercard®.

Once a work order is opened, it is assigned to an implementation staff member who will then reach out to clients to set up a kickoff call.

Still, Visa, MasterCard and Apple® control the actual go-live dates. Once the credit union returns the information needed by the networks and Apple, we submit it to the network. The network setup is currently running 2–3 weeks from time of submission to the beginning of the testing window. The testing window is scheduled for one week and follows a published schedule by the networks and Apple of live dates twice each month.

What's the latest on Apple?

Apple has control of the schedule. There is no appeal or prioritization process with Apple. They are following a "wave" approach: Apple is scheduling live dates the first and third Tuesday of every month. Following the testing period for Visa or MasterCard, Apple requires 7–10 days following that to "make live." Apple has enforced the 95% rule (95% of all an FI's cards must be eligible), and most credit unions are moving forward with both debit and credit when enrolling.

Apple Pay Enrollment

How do we enroll in Apple Pay?

Credit unions need to enroll with their issuer processor. For split-processed clients, Visa and MasterCard have determined that you should enroll with your signature processor.

Your first step is to review the Apple Pay agreement from Apple. If you need a copy of this, please contact your Strategic Relationship Manager.

Once you are prepared to sign the Apple agreement, you can submit a service request for "Apple Pay," located under the "BIN (Cardbase) Changes" listing. You will be put in the queue for implementation and provided with a detailed pre-implementation package.

For a detailed implementation timeline, please access the flow chart here (PDF):
http://co-opfs.org/media/201252/apple_pay_implementation_timeline_infographic.pdf

Apple Pay Details

How do members load their card into Apple Pay?

There are a number of ways members can load a card in Apple Pay. If it is a card on file in iTunes®, Apple Pay will present that card as a choice. Or the member can manually enter their card, or take a picture of the front of the card, which will read the cardholder data and send it to the TSP. The actual picture is not added to the camera roll nor is it stored in iCloud®.

How is the cardholder authenticated in Apple Pay?

When the cardholder adds a card to Apple Pay, both Apple and the network run the request through a number of risk parameters to ensure that the requester is indeed the valid owner of the card. This may include things like history in iTunes, address verification or other authentication requests. These requests will use existing infrastructure to send through things like a zero auth request, AVS request, etc. If it passes, the card will be tokenized and enabled on the phone.

If however these checks fail, the cardholder will go into what is called "yellow path" authentication. In this scenario, the cardholder is directed to call their credit union, which will need to authenticate the cardholder using its current authentication protocols. The credit union will then need to go to the Life Cycle Management portal to "release" the token so that it can be sent to the member.

What is a Life Cycle Management portal?

Each of the networks, Visa and MasterCard, provide an online portal that allows you to manage the life cycle statuses of tokens, such as disabling or resuming a token. CO-OP will provide details of how to get access to this tool during your enrollment.

What is token Life Cycle management?

Token life cycle management is the process of managing the status of the token based on various events such as a PAN being lost or stolen, mobile device being lost or stolen, etc. A token can go through various life cycle status updates such as Active, Suspended, Deleted during the course of its life.

What if the token is lost or compromised?

When members contact the credit union, you can disable a token using the life cycle management portal.

Members can also go to Find My iPhone and report the phone as "lost," which will automatically suspend tokens directly with Apple.

Apple Pay Details (continued)

If we hot-card a card, will the token automatically be closed as well?

At this time, you will need to go into the life cycle management portal to delete the token. Support for an automated solution for actions such as deleting a token when a card is closed is on our roadmap.

Will we be able to integrate Apple Pay into our mobile platform?

You can link your mobile banking platform to Apple Pay. Currently this is a one-directional link from Apple Pay to launch your mobile application.

What happens when we reissue cards, will Apple Pay still work?

When you reissue a card, either with a new PAN or new expiration date, you will need to instruct your members to remove their old card from Apple Pay and add their new card back into Apple Pay.

Apple Watch Payment Enablement

What are the requirements for using the Apple Watch?

The Apple Watch will need to be paired with an iPhone. It can be paired with iPhone 5, iPhone 5c, iPhone 6, iPhone 6 Plus, iPhone 6s and iPhone 6s Plus (running iOS 8.2 or later). Bluetooth must be enabled to pair the Apple Watch and the iPhone device. An Apple ID and iCloud account are also required.

How is an Apple Watch paired (also called pinning) with an iPhone device?

First the user will need to launch the Apple Watch app on their iPhone. Then they will tap "Start Pairing" on the main Apple Watch screen. Next they will hold their Apple Watch up to their iPhone's camera so the screen is in alignment with the yellow outline box on the iPhone screen. Lastly, they will need to follow the onscreen instructions provided in the Apple Watch app.

How are cards added to the Apple Watch?

The provisioning on the Apple Watch is performed separately from the iPhone or iPad. The Apple Watch is first unlocked using a passcode and then it connects to the paired iPhone via Bluetooth. Credit union members can access the Apple Watch settings app, scroll down to Wallet & Apple Pay and then select "Add Credit or Debit Card". Apple Watch users will add cards using their iSight camera on their iPhone or they can manually type in their account information. Please note: a card previously provisioned into Wallet & Apple Pay will have to be re-provisioned into the Apple Pay Watch app.

What is the first step for using the Apple Watch?

The Apple Watch first needs to be unlocked. The Apple Watch unlock can be performed in 2 ways:

1. With the watch on the user's wrist, the user enters their passcode on the watch.
2. With the watch on the user's wrist, the user enters their passcode on the paired iPhone, which must be connected via Bluetooth and within range.

Apple Watch Payment Enablement (continued)

How are purchases made using the Apple Watch?

Once the watch is unlocked, the user must confirm that Wrist Detection has been turned on. Next, the user will double click the side button (also called the Digital Crown) on the Apple Watch. They will then see their default card image. They can proceed with the default card or swipe left to right and select an alternate payment card. Once a card is selected, the user will simply hold the display of the Apple Watch within a few centimeters of the contactless reader. A gentle pulse, beep and checkmark on the Apple Watch screen will provide confirmation that a payment has been successfully made.

Are there any security features built into the Apple Watch?

Wrist Detection is a security feature built into the Apple Watch. This feature can detect when a user removes the watch and it prevents the ability to perform transactions until the user puts the watch back on and enters the passcode.

Are there any technical variations for the Apple Watch?

No provisioning or token processing updates are needed to support the Apple Watch. The same information that is taken into consideration for Green Path, Yellow Path or Red Path will apply when provisioning into the Apple Watch app. In each of Visa and MasterCard's token management portals, a new device type, "watch," will be available to your customer service representatives. Transaction history on Apple Watch will be available at a later date.

Does the Apple Watch require any changes in Member support?

Existing authentication procedures will remain consistent when assisting a member with an Apple Watch transaction. It is anticipated that new provisioning requests will initially spike as the Apple Watch can be paired with a broader iPhone selection including iPhone 5, iPhone 5c, iPhone 6, iPhone 6 Plus, iPhone 6s and iPhone 6s Plus. Credit union members using the Apple Watch will need to understand that disabling the Apple Watch passcode, logging out of iCloud, disabling Wrist Detection, or unpinning the watch from their iPhone will delete any tokens that were previously created and they will have to set up their payment card again via the Apple Watch app.

Where can we find information and support for Apple Pay payments using Apple Watch?

Members can visit https://support.apple.com/en-us/HT204506 for details and support on setting up and using Apple Watch for Apple Pay payments.

Tokenization Basics

Will tokenization replace EMV or provide another option?

Tokenization and EMV will secure our payment system together. Think of EMV as the security for a plastic card in a card-present transaction, and tokenization as the security for digital transactions, whether mobile or online. We believe that the two technologies serve different purposes and Apple Pay will propel digital payment security and mobile payments forward.

Are tokens valid for payment at only one specific merchant?

In Apple Pay, tokens are static but unique to a device, such as a mobile phone. But other deployments of tokenization could be specific to a merchant. Each unique transaction using a token carries with it a unique cryptogram, similar to the cryptogram that is used in a contactless transaction. This ensures that if a token is specific to a merchant, it will only be valid at that merchant and not able to be used elsewhere.

Are tokens valid for one payment transaction only?

No. The payments industry has moved away from single-use tokens due to the valid concern that we will quickly run out of unique tokens.

In Apple Pay, a token (for a specific phone) does not change. It is the same token used for all transactions. What changes is a cryptogram, which is different for each transaction and ensures that a token cannot be duplicated and used elsewhere.

Can a PAN have more than one token?

Yes, a PAN can have multiple tokens, which are each specific to a device. For example, if a cardholder has one card account that is used with four different phones, there would be four different tokens from the token vault, one for each phone.

Currently MasterCard allows nine tokens per PAN, Visa allows 99.

How does it protect us from fraud?

Because the token is specific to the device or potentially the merchant, if it is compromised for example on a phone, the token cannot be used online from a PC. And because it is a token and not the true PAN, the rest of the card account is not in jeopardy. The original PAN is not transmitted as part of the token transaction and is not stored on the phone or at a merchant. The member's real PAN remains securely stored in token vaults residing behind firewalls at highly secure payments networks.

This also means that when a token is compromised you only have to disable that one token and will not need to close the card account and reissue new plastic.

Credit unions should see a decrease in e-commerce and m-commerce fraud and its associated costs.

Acquirers, processors and merchants should experience a reduced threat of sensitive cardholder data being usable by fraudsters if compromised.

Tokenization Details

Where is the vault that assigns the token and the real PAN?

The industry is moving toward a model that will initially rely on a vault at each of the international brands, matching the brand on the front of the card, e.g. if the card is a Visa card, the token and PAN will be stored in the Visa token vault.

Apple Pay uses Visa, MasterCard and American Express for tokenization vault services.

What is a TSP?

TSP stands for Token Service Provider. The TSPs we are discussing in this FAQ are Visa, MasterCard and American Express. A token service provider provides a number of services such as:

- Issuer enrollment
- Authentication protocols
- Token request service (called provisioning), providing an entity like Apple the ability to request a token for a new Apple Pay device
- Mapping of tokens to PAN and storing in the secure vault
- Token/PAN exchange to the issuer when a token transaction occurs
- Life cycle management of the tokens

How will tokens be requested? And from whom?

In the Apple Pay deployment of tokenization, the cardholder initiates the request to Apple, who sends the request to the appropriate network. That means that Visa cards would be tokenized by Visa, MasterCard by MasterCard, etc. The token is generated based on a token BIN range specific to each issuer and sent back through Apple to be stored on the phone. From that point on, the true card number is not on the phone, nor in any database at Apple. It is only at the token service provider, e.g. Visa, MasterCard, Amex.

Call Center

Will call center staff need to be trained on Apple Pay?

Yes, any staff who take member service calls will need to be trained on Apple Pay. There are a number of things your staff will need to understand, such as "yellow path" authentication, deleting a token, resuming a token, etc. Your staff will need to have access to the network's life cycle management portal, which we will cover with you as part of your enrollment process. Training will also be provided on the portals by the networks.

CO-OP has created member-facing FAQs for your staff as well.

Will CO-OP provide life cycle management services on behalf of credit unions?

Yes, CO-OP's Member Center does offer call services for members, either to authenticate in a "yellow path" situation, or to take calls from members who have lost their phones or need other assistance with Apple Pay. They will have access to the life cycle management portals for completion of these actions on your behalf. A contract with CO-OP Member Center would need to be signed for this service.

Transactions

How will chargebacks work if I only have a token?

When the transaction gets to the issuer (and issuer processor) the true PAN will be in the ISO message in the same place it is today, so the issuer will be able to do chargebacks just as is done today. As the chargeback goes back through the payment chain it will be converted back into a token so that the merchant processes the chargeback using the token, not the PAN. Apple Pay transactions at a terminal are considered card-present and in-app purchases as card-not-present.

Will the transaction contain all the normal transaction data?

Yes, all the normal transaction data will be present, such as purchase date, location, merchant, etc.

How will I know that a specific transaction was tokenized?

There will be data in existing fields by which you will be able to know that the transaction began as a tokenized transaction.

Do my BINs need to be enabled with EMV or contactless before I can participate in Apple Pay?

No. EMV technology, although similar, uses different cryptography to secure the transaction. And while Apple Pay uses contactless technology at NFC enabled terminals, the cryptography is de-encrypted at the token service providers. Thus an issuer can participate even if their BINs are still magstripe contact only BINs. If your BINs are already EMV, Apple Pay will work using the contactless protocols.

What happens if I don't enroll my BINs?

Once cardholders get the new iPhones and enable Apple Pay, they will be asked to authenticate themselves and their payment credentials for their card. When this request goes to the TSP, the TSP will confirm that the BIN is enrolled. If it is, the token will be provisioned to the phone. If the BIN is not enrolled, the cardholder will not be able to enable Apple Pay with that card.

Will PIN transactions work with Apple Pay?

Yes, they will. In-store Apple Pay transactions will be treated as card-present contactless transactions. Merchants can prompt for PIN (as they can today) but few do. PINless transactions, those under $50 today, will also be supported. Most acquirers do not support PIN today for in-app transactions, so just like in the traditional mag stripe environment, those will remain CNP non-PIN transactions.

The PIN offset is not sent in a contactless transaction, regardless of whether the contactless transaction originates from a card or a phone. So the only way a PIN can be validated is if PIN validation is done against the database at CO-OP or your host. Because of this, credit unions who validate PINs using the data on the magstripe will need to change their authorization method to cooperative processing and begin validating PIN from the database at CO-OP or your host.

Do we need to enroll with our PIN networks as well?

Your BINs will only be "enrolled" in one TSP. If it is a Visa card, you will enroll in the Visa Token Service. If it is a MasterCard card, you will enroll in MasterCard's token service, known as MDES. Enrollment is done through your signature issuer processor.

Regional networks will require you to notify them that you are enrolling your BIN in Apple Pay. This may be called "registering" with the PIN network or simply "adding a BIN" to the network's load file. The new BINs are actually token BINs assigned to your true BINs.

Contact your PIN networks for their specific processes. CO-OP will be assisting credit unions with PIN network paperwork just as we do today.

Compliance

Is Apple Pay Durbin compliant?

Yes, Apple Pay is Durbin compliant. However because each PIN network is in a different state of readiness, each credit union will need to contact their legal counsel as it relates to compliance issues such as Reg. II. It is generally safest to ensure that all transaction types have two unaffiliated networks available.

Apple Pay transaction routing, like contactless or traditional mag stripe routing, is determined by the merchant. Assuming your PIN network is ready and certified with the network and issuer processor, merchants will be able to choose that network, just as they do today.

Will we need to certify for tokenization?

CO-OP's certification, which was completed in 2014, will cover our credit unions. However, some testing is required by Visa, MasterCard and Apple. The amount of testing required varies depending on the network and will be shared during your enrollment process with CO-OP.

Will my core data processor or my credit union need to do any development to support Apple Pay?

At this stage, neither the credit union nor your data processor will need to do any development in order for you to offer Apple Pay. As additional functionality is added in 2017, your core data processor may need to make some changes in order to take advantage of future enhancements.

Consumers and Costs

What do I tell my members who ask about Apple Pay?

Apple Pay has created instant awareness and interest. Keep in mind that although everyone is talking about Apple Pay, it will only be available for those members who have the new iPhone® 6, iPhone 6 Plus, iPhone 6s and iPhone 6s Plus and Apple Watch. That is a fairly small number, but won't stay that way for long.

CO-OP has made a portfolio of member facing Apple Pay materials available on the Marketing Portal, including:

- FAQs
- Statement insert
- Lobby poster
- Online, social and newsletter content
- Sample marketing plan

How much will this cost?

There are costs from Apple and Visa/MasterCard as well as your PIN networks. Those costs are detailed in the contracts with those various organizations. Please submit a pricing service request to CO-OP for CO-OP's fees.

Are these transactions card-present or card-not-present, and will there be any changes in interchange rates?

Apple Pay transactions at an NFC device will be considered a card-present transaction. In-app transactions will be considered card-not-present. There have been no announced changes in interchange rates.

Market

How will this Apple announcement affect all the other wallets in the market?

Most industry analysts expect that the number of wallet providers will significantly compress in the next few years.

Is NFC going to be the standard for all contactless payments?

While NFC got a huge boost by Apple, we expect that other technologies may have use cases that are still viable.

Where will tokenization have the biggest impact?

Visa, MasterCard and American Express introduced tokenization to combat e-commerce fraud and are now extending it to mobile payments. We expect it to have a significant impact on all digital payments, whether they are mobile or e-commerce.

Pay

CO-OP Financial Services
9692 Haven Avenue
Rancho Cucamonga, CA 91730
CO-OPfs.org

Be There. Be More.

CO-OP FINANCIAL SERVICES