



Network Tokenization for Merchants

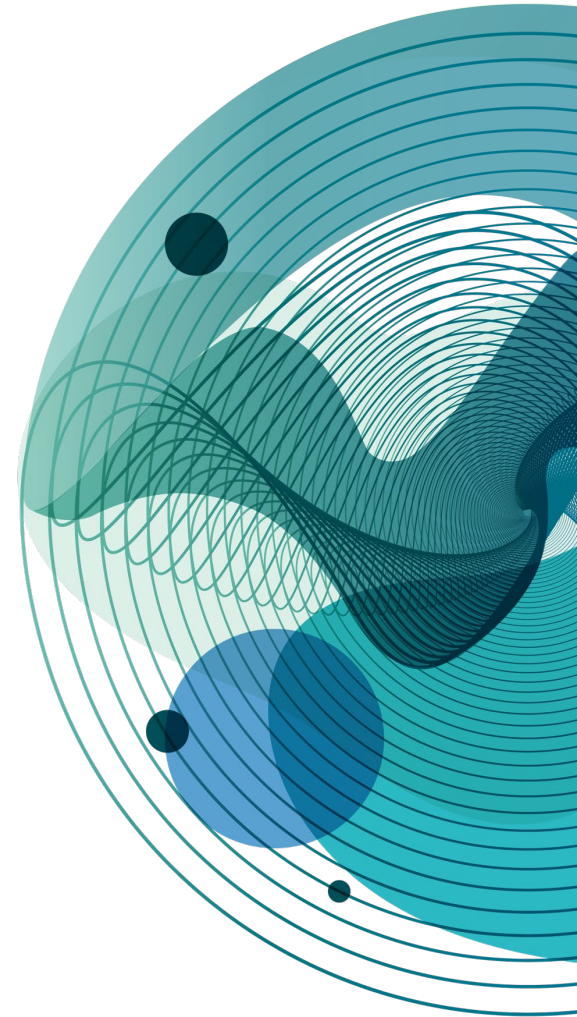
Deloitte Cross-Industry Payments | January 2023

Hosted by:



Table of Contents

- 3** | What is Network Tokenization?
- 4** | Benefits
- 5** | Considerations
- 6** | Incorporating Network Tokenization
- 8** | Payment Account Reference (PAR)



NETWORK TOKENIZATION

Providing value to merchants and consumers while protecting the payment ecosystem

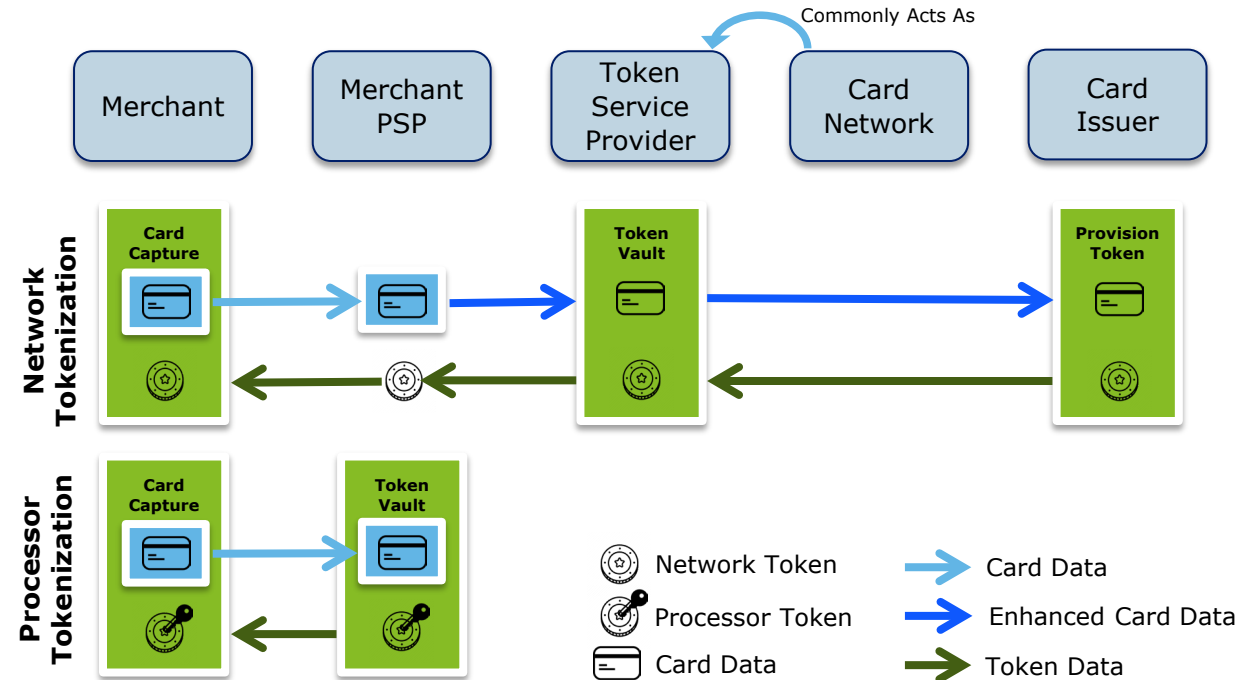
WHAT IS NETWORK TOKENIZATION?

Network Tokenization is an evolution in payment card data protection and transactional services for remote commerce and wallet-based transactions. Network Tokenization is an industry standard published by EMVCo and open to anyone in the payment ecosystem. First introduced with the launch of Apple Pay and the payment networks, Network Tokenization is gaining traction in the Card on File and wallet markets.

PROCESSOR VS. NETWORK TOKENS:





Processor Tokenization is a proprietary service offered by PSPs, Acquirers, and Processors to minimize a merchant's PCI scope. The generated token, which is a replacement for a Personal Account Number (PAN), is restricted to the merchant and PSP limiting its value in the event of a data breach. Network tokenization goes further by generating tokens in cooperation with the Card Issuer and Card Network to offer additional benefits to the merchant and protect the PAN throughout the value chain.

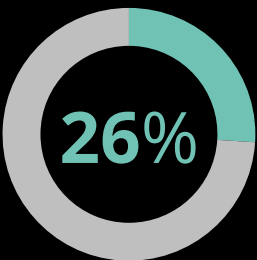
HOW DOES IT WORK?



Depiction of key actors in each token provisioning process

What are the benefits of Network Tokenization?

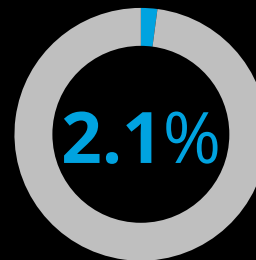
KEY BENEFITS	IMPLICATIONS FOR YOUR BUSINESS	TOKENIZATION IMPACT
 Cost Optimization	Network Tokenization offers cost optimization through two avenues. Visa has recently announced that CNP transactions not using network tokens are expected to be charged 10 Bps higher – an encouragement to use network tokens for CNP use cases. Additionally, storing card data increases security and compliance costs associated with protecting payment data, stopping breaches, notifying customers, and the brand damage a business might suffer in a breach were to occur	Merchants can optimize costs once tokenization has been adopted because of Visa's pricing changes With tokenization, security and compliance costs can be reduced since network tokenization reduces the scope of PCI DSS
 Reduced Fraud	With the pandemic accelerating the expansion of eCommerce and contactless, the number of CNP transactions have increased significantly along with the fraud that can accompany CNP use cases. Businesses must protect themselves from CNP fraud, but also be mindful of declining legitimate customer transactions	To reduce fraud for CNP transactions, network tokens are being implemented as they offer a higher level of security. The impact of any potential data breach is greatly reduced since the data is useless when stolen.
 Improved Authorization Rates	Even minimal increases in authorization rates can lead to meaningful revenue growth. Tokens are issued by networks and banks who have visibility into all activity across the payment life cycle, so the issuers can decision better on all transactions. Since the token can be updated dynamically and doesn't expire, when PANs change, reoccurring charges that are declined due to old incorrect card information will automatically be updated reducing false declines and unnecessary churn on reoccurring revenue	Network tokenization involves card issuers unlike processor tokenization. Network tokens can be limited in scope and offer additional detail about the payment,. This visibility enables them to approve more transactions due to increased involvement, data, and security.
 Better Customer Experience	Customers are providing merchants with card data for card-on-file payments more often than ever presenting businesses with additional challenges. Manually updating card information, dealing with disruptive card re-issuance events like stolen or lost cards can create additional steps for a customer, creating friction at checkout	Card issuers can update network tokens in real time replacing the need for card members to update the information periodically reducing merchant outreach which can lower operating costs.



Decline in Overall Fraud Rates¹

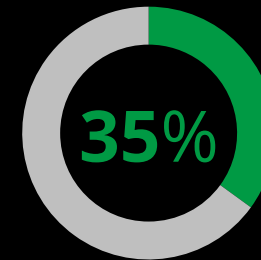
10 Bps

On average, Visa is expected to charge lower rate when using network tokens¹



Increase in average authorization rate¹






Based on volume can increase merchant revenue by millions of dollars



Cardholders stop shopping after one decline²

What should be Considered prior to Implementation?

*Network Tokenization has its benefits, however businesses should understand there are **impacts to consider***

	 Token Provider Lock-in	 Not for Card Present Transactions	 Expect Inconsistency	 Comprehensive Fraud Strategy	 Stick instead of Carrot
Merchant Implications	Consider using a gateway or third-party TSP if you are considering a multi-acquirer ecosystem.	Two different types of tokens may make analytics harder. This can be avoided by either using Processor Tokens for all channels or using PAR to identify customers instead.	Not all issuers support Network Tokens yet, so you may continue to receive multiple token types. This can have an impact on your analytics capabilities. Consider using PAR for analytics.	You should employ a comprehensive fraud strategy to cover areas of the payment ecosystem that Network Tokenization does not protect, such as Account Takeover fraud or card validation bots.	You may have to incur additional cost for not using Network Tokens if your customers are using Visa cards for CNP transactions. Other card networks may implement similar strategies.
Background	Processor Tokens binds a merchant to a processor who is generating its tokens. Similarly, Network Tokens require a Token Requestor ID, which would be assigned to your token provider, such as your processor, thus continuing the lock-in.	Network Tokens are only available for Card Not Present (CNP) transactions, such as e-commerce purchases, Digital Wallets and QR Code based payments. Merchants still need Processor Tokens for in-store Card Present (CP) transactions.	It takes time for the market to fully adopt new technologies such as Network Tokenization. There may be issuers who do not yet support Network Tokens which results in needing a stand-in, such as Processor Tokens or PAR.	While Network Tokenization has several benefits for protecting the merchants and transactions, it does not include protection for all aspects of a payment ecosystem.	Visa has implemented a penalty up to 10 basis points for not utilizing Network Tokens for CNP transactions. Merchants are not being given the choice to adopt Network Tokenization based on their needs, but via coercion.

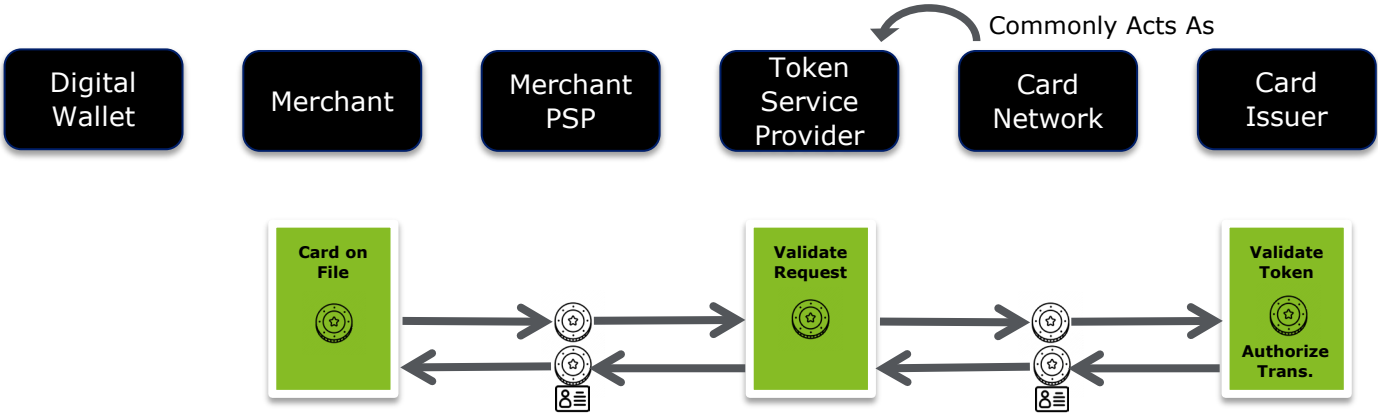
Incorporating Network Tokenization – Digital Channel Use Cases

Merchants use tokens to protect cardholder data. Network Tokens were designed for cards provisioned for wallets, card on file purchases and businesses relying on a subscription revenue model.

Website

Customers utilize previously entered card information for Card on File or Subscription payment transactions. Network Tokens are used to maximize the effectiveness of Card on File transactions.

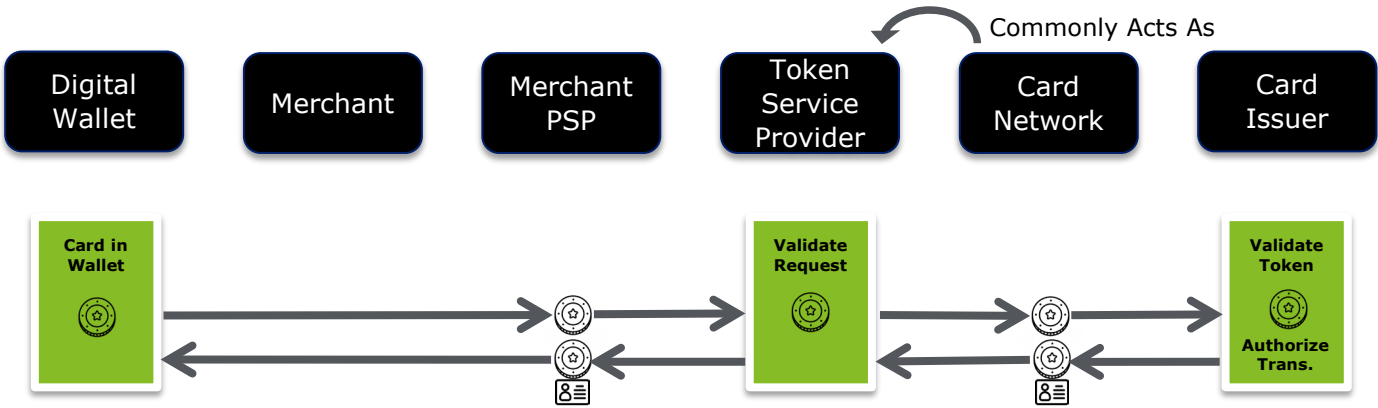
Token information is captured by the merchant and shared with the Token Service Provider and Card Issuer to validate the token and authenticate the transaction. Card Issuer then shares PAR along with the token to complete the transaction.



In-App

Customers purchase goods or services through in-app payment flows or through various digital wallets. Network Tokens are leveraged to complete and secure the transaction.

Token information is shared from the digital wallet with the token service provider and card issuer to validate and authenticate the requests. Card Issuers authorize the transaction and share customer PAR information back to the merchant PSP along with the token.



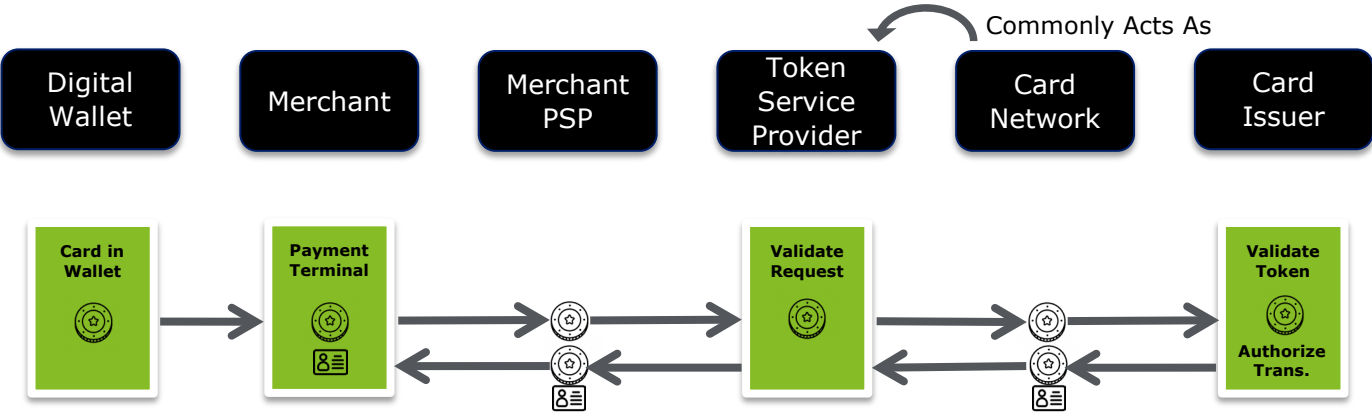
Incorporating Network Tokenization – In-Store Channel Use Cases

Merchants use tokens to protect cardholder data. Since Network Tokens were not designed for card present transactions, not all retail use cases qualify. Merchants that accept physical cards should consider a hybrid token acceptance model or PAR.

In-Store Wallet & QR Code

Customers increasingly leverage wallets like Apple Pay or Google Pay or QR Code-enabled apps for in-store payments. Network Tokens are utilized for these proximity purchases to secure the payment data.

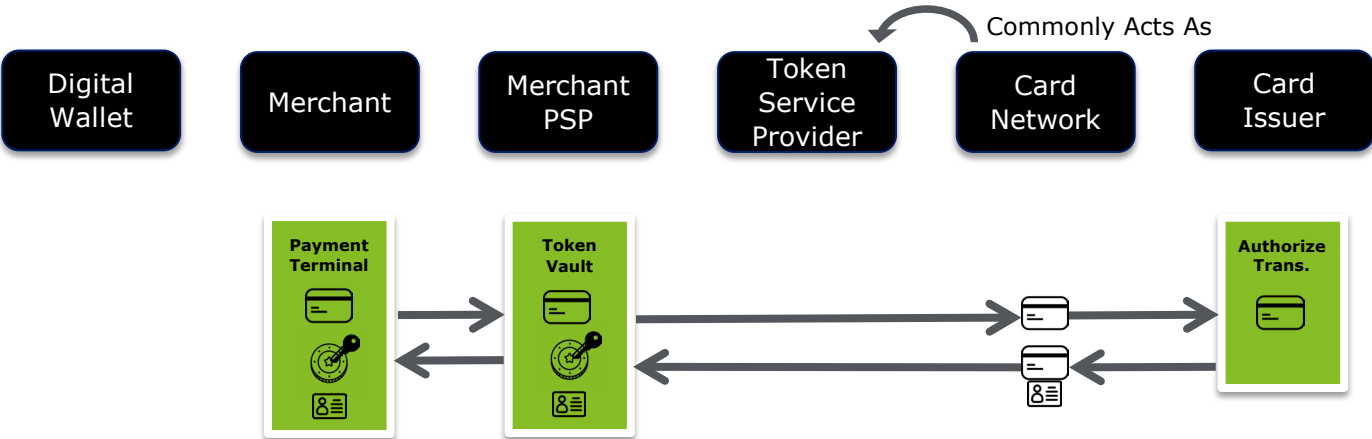
The Payment Terminal captures the token information and shares it with the card issuer, and in return the card issuer shares the PAR information along with the token back to the merchant to complete the transaction



In-Store Card

When customers use physical credit cards, Processor Tokens are still returned in the transaction response as Network tokens are currently not enabled for physical card transactions

The Payment Terminal captures the card data and shares it with the card issuer to authorize the transaction. Card issuers authorize transactions and share with merchants the response and PAR while the processor provides the Processor Token.



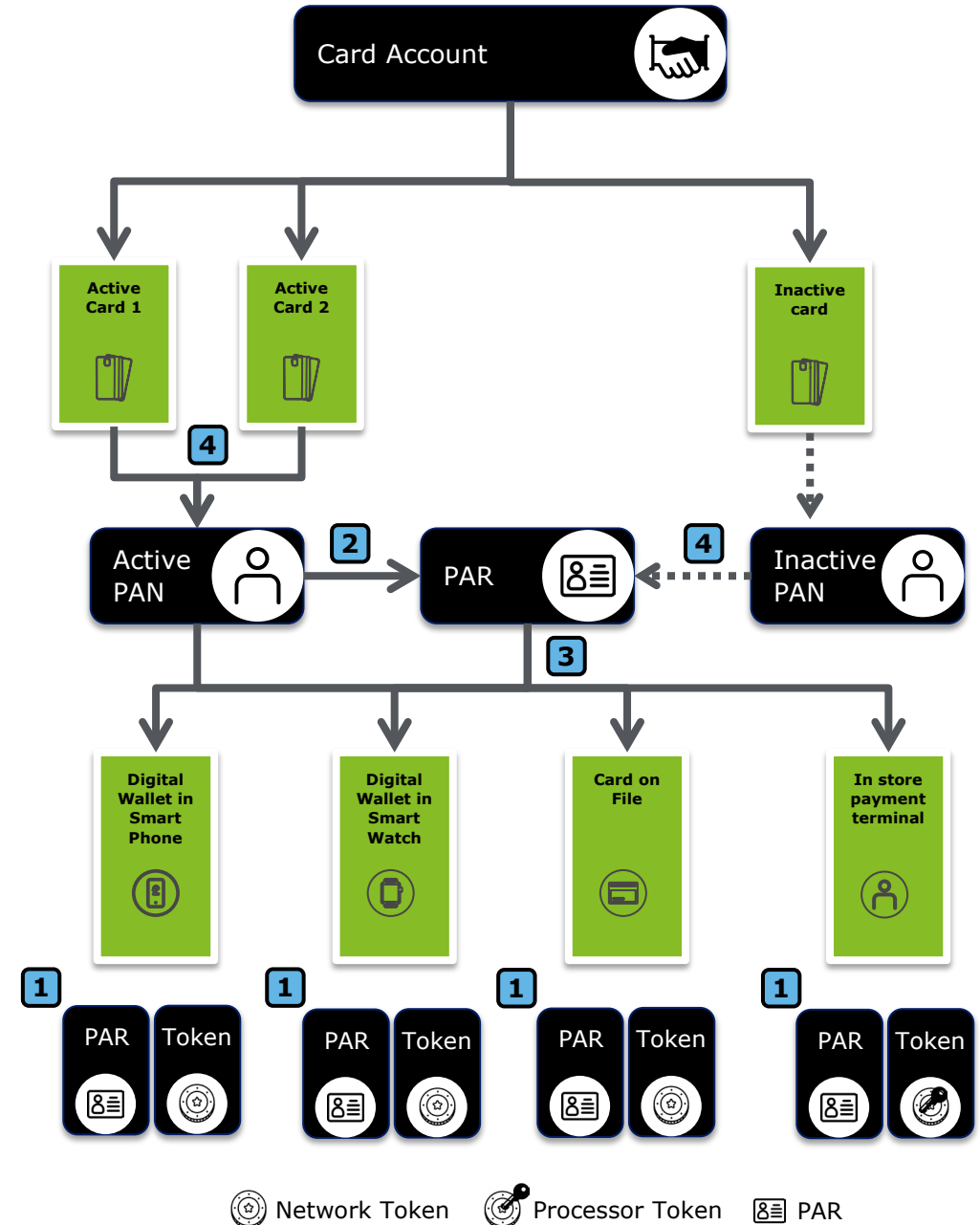
Payment Account Reference (PAR)

What is PAR?

- 1 It is a non-financial value that is non-sensitive and can be used for non-payment purposes such as tracking customers' purchase history across channels and payment instruments
- 2 PARs are linked to the PAN that is associated with the card account; there is a 1:1 link between a PAN and a PAR
- 3 PAR links all PAN and token-based transactions associated with a PAN
- 4 A single PAR exists throughout the life of a card account; even if the PAN changes due to card deactivation or if multiple cards have the same PAN

Benefits of PAR for merchants

- ▶ With increased visibility into a customer's purchase history across channels and payment instruments, merchants can provide targeted value-added services to their customers such as rewards, promotions, and coupons
- ▶ By using a de-sensitized non-financial value for tracking a customer's transactions, the risk of compromising sensitive payment data in the event of a data breach is reduced
- ▶ Since PAR can correlate transactions across different channels and payment instruments, merchants have access to more data which can be used to employ advanced fraud analytics to more accurately identify fraud
- ▶ Merchants can use PARs to augment their Single Customer View (SCV) identifiers for a more robust view into their customer's relationship with the business, resulting in improved customer service and relationship management





For more information, please contact

Conrad M. Sheehan

US Cross-Industry Payments Leader
Principal

Deloitte Consulting LLP
csheehan@deloitte.com

Mark Ericksen

US Cross-Industry Payments
Specialist Leader

Deloitte Consulting LLP
mericksen@deloitte.com

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.