SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE PAYMENTS COUNCIL WHITE PAPER

EMVCo Payment Account Reference (PAR): A Primer

Version 1.1

Publication Date: April 2018

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

The Secure Technology Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Secure Technology Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

Table of Contents

1 Introduction

The tokenization process in payment transactions replaces primary account number (PAN) data with a surrogate value. Use of the surrogate value, or *token*, provides increased protection against fraud and account data compromise by removing the PAN from potentially vulnerable parts of the payments environment. It is important to note that there are several types of tokenization models,[1,2,3] such as acquirer tokenization, security tokenization, issuer tokenization and EMV® payment tokenization.[4]

This paper focuses solely on EMV payment tokenization which is the type of token that's used in mobile wallet transactions such as Android Pay, Apple Pay and Samsung Pay. While payment tokenization has improved the security of the payments ecosystem, it creates challenges for products and services that rely on the PAN to identify a customer's account (such as loyalty and rewards accounts), and for operational services related to a payment transaction (including customer care). For example, before payment tokenization, the PAN could be used to identify a customer's loyalty account.

To address these challenges, EMVCo has introduced a new data element, called the Payment Account Reference (PAR).[5] The Secure Technology Alliance Payments Council developed this white paper to provide a high-level overview of PAR and its use cases for merchants, acquirers, issuers, service providers and other stakeholders. This white paper uses the definitions of payment tokenization and payment tokens from the relevant EMVCo specifications and bulletins cited below. It explains what the PAR is and why it is important, describes how PAR data can be accessed and how the PAR can be leveraged in certain nonpayment use cases, and identifies the impact that PAR may have on key stakeholders.

[1] Secure Technology Alliance, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," white paper, October 2014, https://www.securetechalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/.

[2] EMVCo and Secure Technology Alliance, "EMV Payment Tokenization: What's New," webinar, November 16, 2017, https://www.securetechalliance.org/activities-events-webinar-emv-payment-tokenization-whats-new/.

[3] PCI Security Standards Council, "PCI DSS Tokenization Guidelines," https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf?agreement=true&time=1513278700503.

[4] EMVCo, "EMV® Payment Tokenisation Specification – Technical Framework," September 8, 2017, https://www.emvco.com/emv-technologies/payment-tokenisation/.

[5] "Payment Account Reference (PAR) (Spec Change)" *EMV® Specification Bulletin No. 167*, *First Edition January 2016*, http://www.emvco.com/specifications.aspx?id=23.

2 Overview and Definitions

The PAR is a non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated payment tokens.[6] PAR has a one-to-one relationship with the PAN and a one-to-many relationship with the payment tokens. Figure 1 shows how multiple payment tokens relate to a PAR and the PAN.

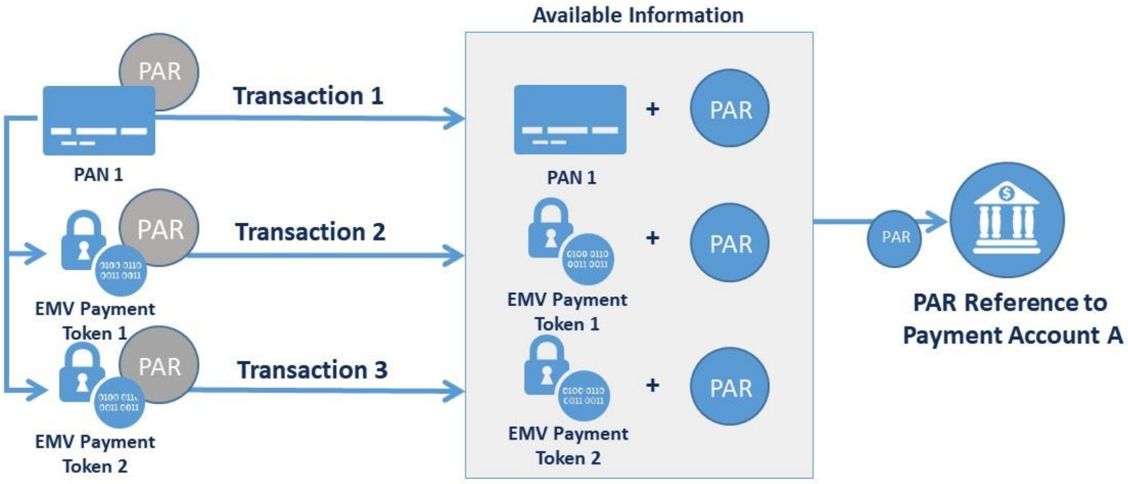

Figure 1. Relationship Between Multiple Payment Tokens, a PAR, and the PAN

The PAR is a fixed-length, 29-character uppercase alphanumeric data element. The first four characters are a BIN Controller Identifier assigned by EMVCo to registered BIN controllers. The remaining 25 characters have unique values.[7] The PAR value is designed to be unique across the global payments ecosystem. A BIN controller may generate the PAR itself or designate a third party, such as a payment network or other entity in the payment ecosystem, to generate it.

PAR data cannot be used to initiate financial transactions; no authorization, capture, clearing, or settlement message can be initiated using a PAR. The guidelines for PAR use also indicate that a PAR value must be generated in such a way that it cannot be reverse-engineered to obtain a PAN or payment token. The PAR data structure is designed to ensure that PAR data cannot be confused with a PAN or payment token. When a replacement PAN is issued for an account, the BIN controller defines whether the PAR changes or remains the same.

Based on the EMVCo definition of PAR, the guidelines for PAR generation, and the intended functions for PAR, PAR data is not considered Payment Card Industry (PCI) account data and is not subject to the requirements for protecting PCI account data specified in the PCI Data Security Standard (PCI DSS). However, PCI DSS applies wherever PCI account data is stored, processed, or transmitted. Therefore, a system is subject to PCI DSS requirements if it stores, processes, or transmits PAR data and also stores, processes, or transmits account data (such as a PAN) or is connected to systems that store, process, or transmit account data.

[6] EMV® Payment Tokenisation Specification – Technical Framework," op. cit.

[7] Additional information on the definition of PAR data element can be found in the EMVCo specification, "EMV® Payment Tokenisation Specification – Technical Framework."

Since payment tokenization replaces the PAN with a payment token, a PAN may not be available as part of the payment transaction data. In addition, there can be multiple payment tokens associated with a single PAN. The absence of PAN data affects nonpayment use cases that rely on the PAN.

Without the PAN in the transaction, PAR provides the ability to identify and link the various payment tokens that map to the same PAN (without having knowledge of the PAN). The PAR data element is uniquely linked to a PAN; depending on how the issuer has set up their environment, a payment account may have multiple PANs, and therefore, each unique PAN will have its own PAR. An example use case is when PAR is generated, linked to a PAN, and then associated with all corresponding payment tokens when the PAN is tokenized. Other use cases are possible.

It is important to consider how PAR is implemented with payment accounts that have a primary account owner and authorized users that are all issued cards. If the additional cards[8] have the same PAN, they will have the same PAR; if the additional cards have different PANs, they will each have a unique PAR.

Figure 2 illustrates how the PAR persists through PAN lifecycle changes.

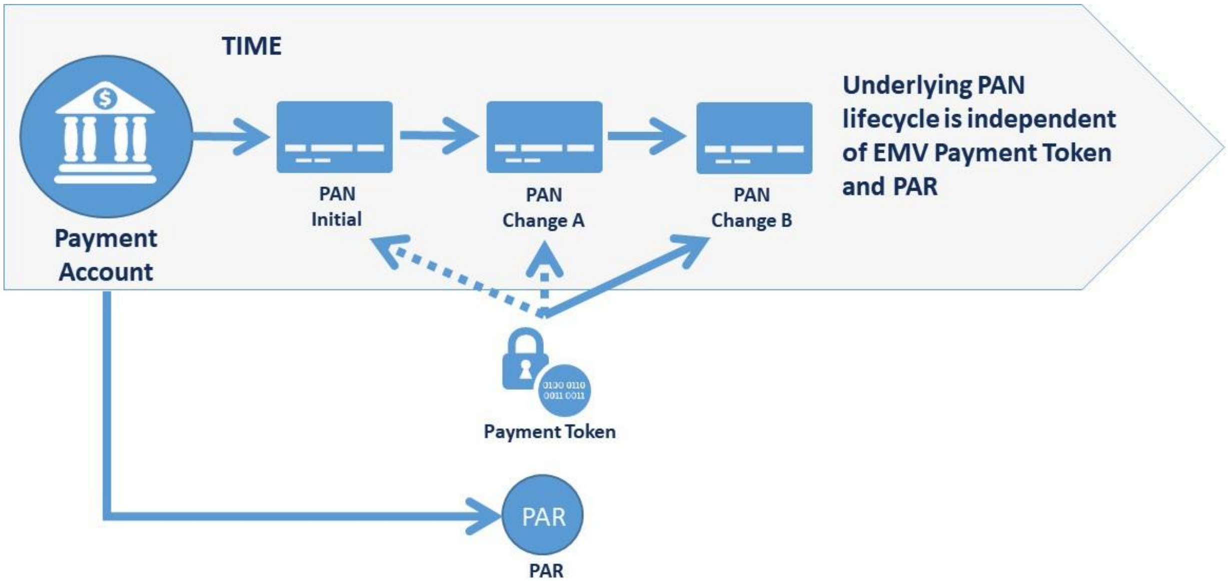

Figure 2. PAR and Lifecycle Management

2.1 PAR Data

PAR data may be provided or used in the following ways:

- As part of a payment transaction, by being populated as part of the authorization response.
- As part of a payment transaction, by being passed from a payment device (e.g., card, mobile phone) to a payment terminal, if the payment device has been provisioned with the payment token and the PAR and if the terminal supports PAR data.
- Using a PAR inquiry service

[8] Additional cards issued to authorized users are sometimes called “companion cards.”

EMVCo has published a set of guidelines for using the PAR that describe how it should fit into the overall payment processing environment. In addition, EMVCo has specified that the PAR can't be used as a consumer identifier, nor used to identify PAN attributes or route transactions. However, each BIN controller is responsible for mandating specific PAR use and working with appropriate entities to incorporate the data element into the message specifications. Acquirers and processors must also implement the changes defined by the BIN controller to be able to make the PAR available to merchants.

2.2 PAR Flow Diagrams

Figure 3 and Figure 4 illustrate how the PAR is accessed during a payment transaction and using an inquiry service, respectively

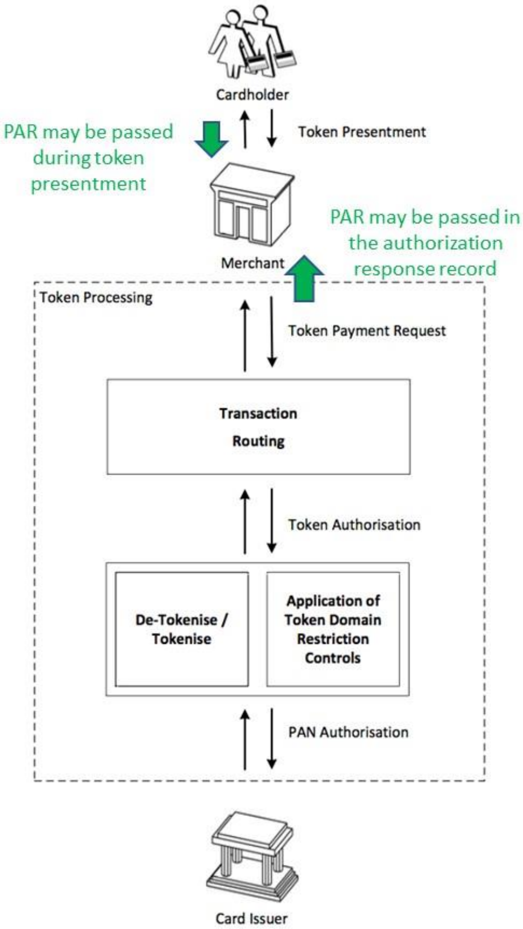

Figure 3. Accessing the PAR during a Payment Transaction

Source: EMV Payment Tokenisation Specification – Technical Framework v2.0

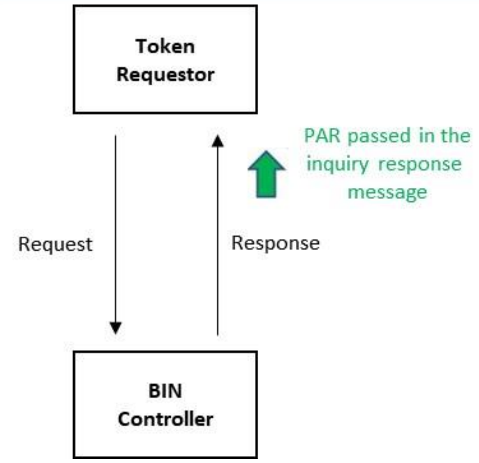

Figure 4. Accessing the PAR Using an Inquiry Service

3 PAR Benefits

As discussed in Section 2, the introduction of the PAR allows for transaction activity to be linked across the PAN and related payment tokens. Using the PAR to link related transactions provides two overarching benefits:

- Enabling the payments acceptance community to execute nonpayment functions in a manner that's consistent.
- Reducing the risks associated with PAN storage.

One of the primary long-term benefits of PAR use is facilitating the payment industry's goal to limit PAN storage within the payment ecosystem.

In general, any application or service that seeks to identify payment activity across payment transactions linked to an account will benefit from using the PAR. This section highlights some of the key benefits that can be derived from use of the PAR.

Reduced Risk

The introduction of the PAR, which is a nonfinancial attribute, enables the payment acceptance community to link transaction activity across related payment transactions without using the PAN. Removing PAN references from systems has the benefit of reduced risk for merchants, and potentially reduced PCI DSS scope when PAN references are completely removed. Further, the PAR cannot be reverse-engineered to get the PAN or payment token, nor can it be used to initiate a payment transaction. These factors make the PAR fit for purpose from a risk perspective when compared to use of PAN as an identifier.

Visibility

As payment ecosystems continue to leverage payment tokenization, the PAR will be the primary mechanism to achieve a consolidated view of transactions associated with a PAN. Systems that are responsible for monitoring limits and thresholds, such as those needed to meet regulatory and anti-money laundering requirements, will benefit from the visibility enabled by using the PAR. Additional data analytics can be run on transaction data which now includes the PAR field.

As an example, when the PAR is used, risk/fraud management systems will have visibility into transaction activity across related payment token-based and PAN-based transaction activity. This has the potential benefit of increasing the effectiveness of such risk/fraud systems in identifying fraud, thereby reducing fraud losses.

New Service Offerings

The introduction of PAR brings the potential for new offerings from stakeholders such as value-added service providers that provide merchant solutions, customer relationship management systems or risk/fraud systems.

Persistence through Lifecycle Changes

The PAR can persist through PAN life cycle changes (e.g., when a payment card is re-issued, and the PAN is changed). If systems previously relied on the PAN as an identifier, those references would need to be updated. The PAR provides better longevity as an identifier that can be used in other relying systems.

Customer Care – Self-service and Agent Servicing

Customer service systems that rely on transaction history and the ability to track various payment devices can benefit from using the PAR. As described in the transit use case (see Section 4.3), the ability to link related transactions to the customer's PAN is valuable for customer service. When a customer calls for assistance and provides the customer service representative with a PAN, a system using the PAR can retrieve all activity associated with that PAN, regardless of what device was used and whether the transaction used a PAN or a payment token. In self-service channels, such as web sites or mobile apps, customers can enter a PAN and the system can leverage the PAR to provide a complete snapshot of transaction history and billing activities.

4 PAR Use Cases

This section describes a variety of use cases for the PAR, for loyalty programs, customer relationship management (CRM), open payment transit systems, and risk management/fraud checking. These use cases are examples; the BIN controller may define additional guidance on PAR uses in addition to those defined by EMVCo. Parties interested in implementing the PAR should check with the BIN controller for guidelines on allowable uses.

The following use cases are meant to be examples; they are not all-inclusive.

4.1 Loyalty Programs

Merchant-based loyalty programs traditionally rely on a dedicated loyalty card. The loyalty card is presented during a purchase to obtain points or rewards that can be applied to future purchases. Loyalty cards support a tender-neutral relationship between a customer and a merchant, allowing customers to benefit regardless of whether they use a payment card (and if so, which one) or whether they pay with cash.

Alternatively, certain merchants can recognize a customer based solely on the payment card used and not have a specific loyalty card. In some cases, loyalty accounts can be proactively linked to a specific payment card, or a merchant may choose to build a customer profile and provide rewards based solely on the payment card account. The advantage of these approaches is that they eliminate the need to present a separate loyalty card at payment. The disadvantage is that receiving benefits is tender specific.

4.1.1 Issues with Loyalty Program Implementations

Card re-issuance and PAN lifecycle events often impact the ability of a merchant to identify a customer’s loyalty account based on the PAN.

In addition, since multiple payment tokens may be linked to a single PAN (e.g., if there are domain-specific tokens), payment tokenization threatens to impact payment-card-linked loyalty programs for merchants. For example, the payment data provided to the POS by presenting a physical EMV chip card will be different than the data provided when using a mobile wallet in which that same physical card has been loaded and tokenized. Once payment tokenization becomes commonplace, merchants, acquirers, and third-party loyalty program providers will no longer be able to rely on consistent PAN data to recognize returning customers.

Widespread use of payment tokens may force many merchants to return to dedicated loyalty cards, reducing customer convenience.

4.1.2 Leveraging the PAR in Loyalty Programs

A PAR can be used to reestablish an effective payment-card-linked loyalty program and preserve simplified recognition of customers. The merchant can use the PAR to recognize a particular customer’s PAN across multiple commerce domains and payment tokens.

Once PAR use is commonplace, merchants can leverage the PAR to create or enhance an “automatic” loyalty program for customers. However, note that use of the PAR does not address one limitation common to any card-based loyalty program; it is not tender neutral. PAR data is tied specifically to the PAN.

4.2 Customer Relationship Management

Many merchants invest heavily in CRM programs. These programs include services such as the following:

- Merchandise returns
- Customer service and support
- Delivery of offers and promotions

4.2.1 Impact of Payment Tokenization

Like loyalty programs, good CRM programs are not channel specific; they identify customers regardless of whether the customer is making a web, in-store, or mobile purchase. Multichannel CRM programs often rely on the card number used for the purchase to identify the customer. Card numbers help merchants quickly identify customers (or previous purchases made by a specific customer), providing improved service and ultimately strengthening customer loyalty. As is the case for loyalty programs (Section 4.1), however, card re-issuance, PAN lifecycle events and the use of payment tokens make this approach to CRM more difficult to manage.

4.2.2 Leveraging the PAR in CRM Programs

The ability for customers to use multiple payment devices (such as smartwatches, NFC-enabled phones, and wearables) in place of a single payment card, combined with the introduction of payment tokenization, has created challenges for merchant CRM programs that rely on the PAN. The merchant can use a PAR to link a specific PAN and its affiliated payment tokens across multiple commerce domains.

Once use of a PAR is commonplace, merchants can leverage it to create or enhance their CRM programs. However, note that use of the PAR does not address one limitation common to any card-based CRM program; it is not tender neutral. PAR data is tied specifically to cardholder's PAN.

4.3 Transit Open Payments

In a transit open payments system, riders can use an open-loop contactless product (e.g., a contactless bank card or a payment account credential used with an NFC-enabled mobile device) to access the transit system. The card or device may pass a payment token to the contactless reader at the entry point. There are two main approaches for how transit systems will process fares when an open-loop contactless product is used, and a given agency may use one or both. One method is for the transit agency to aggregate all ride activity into a single financial transaction. In the second method, the contactless payment credential is linked to a transit account (and pre-purchased fare product) in the back office. In transit open payments systems, a PAR could be useful for fare processing, customer service, and lifecycle management.

4.3.1 Leveraging the PAR in Fare Processing

In a transit system that accepts bank-issued contactless products as fare media at points of entry, the fare system must be able to identify each individual card or payment device (e.g., mobile phone, wearable). There is additional value in being able to link multiple cards or payment devices that are linked with a single PAN.

The payment token by itself should be enough to identify a specific card or device, since the token is a unique value. A transit system can use the PAR to link multiple cards or other devices with payment tokens that are linked to the same PAN, enhancing the rider experience and potentially enabling new transit products. The transit agency could also use the PAR to aggregate transactions or allow riders to link multiple form factors to a single transit account. For example, an NFC-enabled smartphone equipped with a mobile wallet, a smart watch with contactless payment capability, and a contactless payment card – all with unique payment tokens – could all be linked to the same PAN and have the same PAR. The rider could then decide which form factor to use based on the rider's destination or other criteria. However, this application could raise concerns about potential fraud, such as multiple users accessing a single time-based transit product on different devices. In this case, depending on agency policy, the PAR could instead be used to prevent or limit the use of more than one form factor.

4.3.2 Leveraging the PAR for Customer Service

Customers can access transit systems using devices such as mobile devices or smartwatches, which have replaced the PAN with a payment token that may be unknown to the customer. In this scenario, only the payment token and not the PAN is processed within the transit merchant's system. The ability to link these tokenized transactions to the customer's PAN is valuable for customer service. When a customer calls for assistance and provides the customer service representative with a PAN (as the customer won't know the payment token), a system using the PAR can retrieve all activity associated with that PAN, regardless of what device was used. In the case of an anonymous account (e.g., where the rider has not registered with the transit fare system), using PAR might be the only way to identify customer activity.

In self-service channels, such as a web site or a mobile app, where a PAN is entered by the customer, the system can leverage the PAR to provide a complete snapshot of ride history and billing activities.

4.3.3 Leveraging the PAR for Lifecycle Management

When customers use open-loop contactless products as transit fare media, it is important to create a reliable link between the customer's transit account and the form factor. But form factors can be replaced, creating complications. For example, when a customer replaces a mobile phone and recreates a mobile wallet on the new phone, the payment token provisioned to the new phone may not be the same. If a new payment token is provisioned, the transit system can leverage the PAR to link the new payment token to the customer's current transit account and ride activity.

4.4 Merchant/Acquirer Risk Management and Fraud Checking

Merchants and acquirers may have implemented risk management systems based on PANs. Managing risk becomes challenging when transactions that involve payment tokens and transactions that involve a PAN are comingled. When only the PAN is used, the merchant and acquirer can see all transactions conducted with a particular PAN. When transactions are conducted using payment tokens, visibility is lost.

When all transactions involving a PAN and its payment tokens are combined using PAR, merchants and acquirers must perform certain actions to determine aggregate risk levels and manage fraud:

- The fraud system needs to be able to access the PAR (either as a data element from the payment device or in the authorization response message or through an inquiry function).
- Merchant POS and transaction systems must be upgraded to support the use of the PAR.
- Merchant and acquirer fraud management solutions may use the PAR as a replacement index value for the PAN.

5 Impact of the PAR on Key Stakeholders

Use of the PAR affects numerous key stakeholders in the financial payments ecosystem, including:

- Merchants
- Acquirers
- Service providers
- POS and payment terminal providers
- Issuers
- Payment networks
- Token service providers (TSP)
- Token requestors

This section describes the effects of PAR use on each stakeholder group that implements the PAR and indicates where there may be challenges.

Before the PAR can become a standard element in transactions, all parties within the merchant-acquirer ecosystem must implement message format changes, including: merchants, independent sales organizations (ISOs), value-added resellers (VARs), and software providers. For some period of time, stakeholders need to expect that the use of the PAR will not be ubiquitous and that systems will need to accommodate this. The PAR is sent to the acquirer in the merchant's authorization request message in tag 9F24, as a subset of data element 55. For traditional magnetic-stripe swipe transactions, the acquirer receives the PAR in data element 56 of the authorization response message.

5.1 Merchants

Support for the PAR is subject to BIN controller and third-party requirements for implementation, which may differ by BIN controller. If a merchant chooses to support PAR, its use can require merchants to update software and processes and be dependent on support at acquirers, gateways and processors.

The PAR is introduced into an EMV transaction in new tag data (9F24). For a non-EMV transaction, the PAR is added as part of the standard ISO transaction data (e.g., in an authorization response).

Depending on BIN controller and other third-party requirements, merchant considerations include:

- Support for the PAR in both authorization request and response messages
- Updates to POS software and terminals
- Updates to other back-office and customer support systems (e.g., those that support loyalty programs)

5.2 Acquirers

Support for the PAR is subject to BIN controller and third-party requirements for implementation, which may differ by BIN controller. Depending on BIN controller and other third-party requirements, acquirer considerations include:

- Updates to systems processing authorization so that they include PAR data
- Impact of updates to POS terminal code
- Updates to systems implementing fraud screening, chargeback and other value-added services

- Updates to other systems (e.g., data analytic tools, merchant transaction research)

Acquirers will need to send the message format changes to every merchant, ISO, VAR, and software provider and provide them with updated message format specifications. All affected parties will then need to complete some type of testing to ensure proper PAR implementation.

5.3 Service Providers

Service providers of loyalty, CRM, or risk/fraud management services who elect to work with PAR data will be required to make changes to their systems. They will need to upgrade systems to handle the new PAR data field, link a PAR to a PAN, and expand their APIs.

The PAR is an additional data element. While in many systems adding another field may not be a challenge, significant costs may be incurred in meeting the requirements for testing (new tools to support the additional field), and implementation of new APIs and interfaces.

Considerations for service providers include:

- Coding changes to switch from using the PAN to the 29-character PAR as an index for services
- Impact of updates to POS terminal code
- Update to risk/fraud management systems to include PAR data

5.4 POS and Payment Terminal Providers

Payment terminal providers will be impacted by the introduction of the PAR to the payments and value-added ecosystems. Software and APIs will need to be updated to accommodate the additional data and provide backward compatibility.

The PAR is a new data field that can be transmitted to a payment terminal from a payment device. For the data to be interpreted correctly, the software running on the payment terminal must be able to request, recognize, and parse the PAR data properly. Modern payment terminals have software architectures that allow rapid change to higher level functions (e.g., video display graphics, user prompts). However, the software that decodes data coming from the payment instrument is lower level code that changes less often, as the specifications from the payment networks and EMVCo are relatively stable. This lower-level software will most likely need to change to accommodate PAR use. Further, PAR data capture for EMV transactions will be in tag 9F24. For non-EMV transactions, PAR data capture will likely vary by BIN controller, further affecting the amount of lower-level code that must be changed.

For most payment terminals, the API through which data is passed to the POS (for integrated architectures) or the acquirer network (for standalone architectures) will need to be updated. A new field may need to be defined within the API and the characteristics of that field communicated to POS designers and system integrators. In the case of standalone architectures, acquirers will probably define how the PAR data should be presented to their networks, and the payment terminal software will need to be updated to implement the required changes.

Updates to lower-level payment terminal code are infrequent and releasing updates can be complicated. Updating terminal code affects merchants, POS providers, integrators, acquirers, and service providers, and interrupts store operations. Some merchants can push updates to all terminals from one location. Others will need to replace terminals or download new code to the terminal at each POS individually. Both methods involve challenges, and it will probably take time for PAR-compliant code to be deployed widely.

POS hardware and software providers will likely need to upgrade their software solutions to accommodate PAR data. As outlined in Section 2, PAR data will need to be handled in the traditional authorization request/response between the merchant's POS and the acquirer. It may also need to be handled for new requests, such as for a PAR inquiry which could originate at a merchant POS for managing a loyalty program or handling a CRM event.

Most POS systems also provide the primary point of entry for data related to loyalty and/or CRM transactions. If a merchant's POS contains code to leverage a tokenized PAN for a loyalty card, then that code will need to be significantly modified to support the use of the PAR for that same function. Lastly, both POS and payment terminal providers will need to accommodate the co-existence of the PAR and PAN/payment-token-related solutions; the transition will likely span several years until all payment devices have PAR data associated with them. Implementation demands flexible software solutions with strong backward compatibility.

5.5 Issuers

Support for PAR is subject to BIN controller and third-party requirements for implementation, which may differ by BIN controller. Issuer systems may be impacted to accommodate PAR use. The level of impact will depend on the issuer's level of adoption. At a minimum, issuers will need to ensure that their systems can accept PAR data in the authorization message and provide both the new PAN and the current PAR to the BIN controller or third party for lifecycle events (e.g., when a PAN changes).

Depending on the issuer's level of adoption of PAR, other considerations may include:

- Changing the provisioning and personalization processes and message formats to allow for the PAR value in tag 9F24.
- Enhancing back-office processes for chargebacks and fraud systems with functionality to support and retain the PAR.
- Managing the lifecycle of product portfolios for transitioning to PAR use.

When a PAN changes, issuers must be able to provide the updated and old PAN to the BIN controller or third party that maintains the PAR mapping. A new process may be needed to link a PAR to all applicable payment tokens for each PAN (either at the issuer or at the BIN controller). Creating the internal standards needed to ensure compliance with all of the BIN controllers will require significant time.

As PAR deployments continue to grow, it is conceivable that PAR data will be personalized on EMV chip cards and dual-interface cards. If an issuer wanted to support this, PAR data would need to be incorporated into the EMV card data preparation and personalization processes. The method for adding PAR into the card personalization process may vary, depending on whether the issuer is also the BIN controller.

5.6 Payment Networks

Payment networks are operators of electronic systems used to accept, transmit or process transactions made by payment cards and transfer information among card issuers, acquirers, payment processors, merchants and cardholders for one or more payment systems.

In conjunction with the BIN controller, a payment network will need to make updates to messaging requirements in order to support the PAR and to communicate the changes to all entities connected to or utilizing the payment network.

Considerations for payment networks include:

- Understanding any specific requirements for the PAR that the BIN controller may define.
- Ensuring an ISO-defined field for PAR data is available in message specifications, which may include authorization, capture, clearing and exception messages.
- Defining where the PAR is included as an EMV tag (9F24) and ensuring that it is passed along with other EMV tag transaction data in data element 55 within authorization, capture, clearing and exception messages.
- Making the PAR field available to acquirers and payment processors in authorization transaction responses.

5.7 Token Service Providers

Token service providers (TSPs) will be involved in the provisioning of the PAR with a payment token, enabling the passing of the PAR in response to a successful payment token request and supporting detokenization.

Considerations for TSPs include:

- Understanding any specific requirements for the PAR that the BIN controller may define.
- Ensuring that their interfaces for payment token requests can support the provisioning of PAR data to a token requestor as part of a successful payment token request.
- Ensuring the PAR data is correctly provisioned based on whether the payment token will be used by an EMV-based application utilizing EMV tag 9F24 or a non-EMV-based application which should use an appropriately defined field for PAR date and not EMV tag 9F24.
- Where a TSP supports detokenization services to specific authorized entities, providing a method for providing PAR data as part of the detokenization response

5.8 Token Requestors

Token requestors will request and receive PAR as part of the process for provisioning or storing a payment token. Token requestors may be independent token requestor services, gateways, merchants, OEMs, wallet providers, account updater services, or other payment ecosystem participants, provided they are registered with a TSP.

Considerations for token requestors include:

- Understanding any specific requirements for the PAR that the BIN controller may define.
- Receiving the PAR via TSP interfaces for token requests.
- Storing and/or passing the PAR data element, as appropriate.
- Transmitting the PAR in the appropriate data element/field as part of the payment transaction process.

6 Conclusions

Payment tokenization was introduced to enhance the security of processing payments across card-present and card-not-present channels by reducing PAN exposure. While payment tokenization has improved the security of the payments ecosystem, it has created challenges for products and services that rely on the PAN. The PAR was defined by EMVCo to ensure that payment processing and value-added services which currently rely on PAN can continue to be delivered seamlessly and reliably in a tokenized payment environment.

In order to realize the full potential of the PAR, however, it must be part of all payment interactions; all impacted stakeholders will need to support PAR data across all channels and across PAN and payment token usage. While the PAR was designed for tokenized transactions which, to date, have been primarily used for mobile payment and e-commerce transactions, ubiquitous use would also cover EMV chip cards and legacy magnetic-stripe systems. There may also be instances where PAR adoption is voluntary. Additionally, since BIN controllers specify the allowable uses of PAR, consistency across the various BIN controllers will benefit the payment acceptance community and help to streamline PAR implementation.

It is also important to note that EMVCo specifications limit the use of the PAR to returns, chargebacks, fraud risk analysis, regulatory needs (such as anti-money laundering), and non-payment related purposes, as defined by the BIN controller. The PAR is not considered PCI data: the PAR for each PAN is unique and cannot be reverse engineered to identify the PAN or any affiliate payment tokens. It is important as PAR implementation becomes more widespread to be conscious of potential privacy concerns and avoid applications that could be viewed as compromising consumer privacy. It is therefore important for service providers to avoid using the PAR beyond the scope defined by EMVCo and the BIN controller and be cognizant of local or regional regulations.

It is expected that many next generation payment devices will leverage payment tokenization. The PAR was designed to play an important role in providing the ability to link multiple payment tokens with a PAN. The Secure Technology Alliance recommends that all payments industry stakeholders become familiar with the PAR and assess how it can solve current challenges and support future requirements.

7 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Payments Council to provide a primer on the EMVCo Payment Account Reference (PAR), document expected use cases for the PAR and describe the impact of PAR implementation on key payments ecosystem stakeholders.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance wishes to thank Council members for their contributions. Participants involved in the development and review of this white paper included: American Express; Capital One; CPI Card Group; First Data; JPMorgan Chase; Mastercard; Metropolitan Transportation Authority (MTA); Rambus; Tri County Metropolitan Transportation District of Oregon (TriMet); TSYS; Visa; Worldpay.

The Secure Technology Alliance the Council members who participated in the project team to write the document, including:

- **Clinton Allen**, American Express
- **Roberto Cardenas**, TSYS
- **Simon Dix**, Mastercard
- **Jack Jania**, Independent
- **Christine Lopez**, Worldpay
- **Chris Marconi**, Capital One
- **Joshua Martiesian**, MTA
- **Cathy Medich**, Secure Technology Alliance
- **Sadiq Mohammed**, Mastercard
- **Keith North**, CPI Card Group
- **Tony Sabetti**, JPMorgan Chase
- **Rhyan Schaub**, TriMet
- **Chandra Srivastava**, Visa
- **Sridher Swaminathan**, First Data
- **David Worthington**, Rambus

Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners. EMV® is a registered trademark of EMVCo.

About the Secure Technology Alliance Payments Council

The Secure Technology Alliance Payments Council focuses on securing payments and payment applications in the U.S. through industry dialogue, commentary on standards and specifications, technical guidance and educational programs, for consumers, merchants, issuers, acquirers, processors, payment networks, government regulators, mobile providers, industry suppliers and other industry stakeholders.

The Council's primary goal is to inform and educate the market about the means of improving the security of the payments infrastructure and enhancing the payments experience. The group brings together payments industry stakeholders to work on projects related to implementing secured payments across all payment channels and payment technologies. The Payments Council's projects include research projects, white papers, industry commentary, case studies, web seminars, workshops and other educational resources.

Additional information on the Payments Council can be found at https://www.securetechalliance.org/activities-councils-payments/.

8 Appendix A: Glossary

BIN Controller	Entity that determines the rules for use of the Issuer Identification Number (IIN) under their control.[9]
Payment Account Reference (PAR)	A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated payment tokens.
Payment Network	Operator of an electronic system used to accept, transmit or process transactions made by payment cards and transfer information among card issuers, acquirers, payment processors, merchants and cardholders for one or more payment systems.
Payment Token	A surrogate value for a PAN that is a variable length, ISO/IEC 7812-compliant numeric issued from a designated token BIN or token BIN range and flagged accordingly in all appropriate BIN tables. A payment token must pass basic validation rules of a PAN, including the Luhn check digit. Payment tokens must not collide or conflict with a PAN.[10]
Payment Tokenization	A specific form of tokenization, specified by EMVCo, whereby payment tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs as described by the processes defined in this technical framework.[11]
Token Service Provider (TSP)	Entity within the payments ecosystem that provides registered token requestors with 'surrogate' PAN values, otherwise known as payment tokens by managing the operation and maintenance of the token vault, deployment of security measures and controls, and registration process of allowed token requestors.[12]
Token Requestor	Entity that initiates requests that PANs be tokenized by submitting token requests to the token service provider.[9]
Tokenization	Process by which a placeholder or surrogate (payment token) is substituted for a PAN. Typically, tokenization is a service offered by a payment network, acquirer, token service provider or third-party service provider.[13]

[9] EMVCo, op. cit.

[10] EMVCo, op. cit.

[11] EMVCo, op. cit.

[12] "Mobile and Contactless Payments Glossary," U.S. Payments Forum, September 2017, http://www.uspaymentsforum.org/mobile-and-contactless-payments-glossary/

[13] "Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud," U.S. Payments Forum, July 2016, http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud-webinar/