How Emerging Data Elements Can Support Mobile Wallet Use Cases

Version 1.1

Publication Date: November 2019

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV® is a registered trademark of EMVCo, LLC in the United States and other countries around the world.

Version 1.1 – Update to Table 3. Payment Network Support for PAR

Copyright ©2019 U.S. Payments Forum and Secure Technology Alliance. All rights reserved. Comments or recommendations for edits or additions to this document should be submitted to: info@uspaymentsforum.org.

Table of Contents

1. Introduction

As issuers and merchants implement new and innovative payments technology, consumers can select from a myriad of payment experiences while purchasing goods and services. Consumers have never had so much choice in payment options. Card-present interactions can now be conducted using various device-centric form factors resulting in the need for payment stakeholders to augment existing or create new transaction types. Consumers are empowered with information and payment options at their fingertips and can purchase goods and services by clicking a button or by placing a mobile device or wearable in close proximity to a point-of-sale (POS) device. This ongoing evolution has required the payments industry to introduce new data elements to allow the new form factors to be used in the payment or commerce cycle.

The number of options supporting both physical card and digital card-present transactions has increased in recent years. While card-not-present digital transactions (e.g., digital wallets, remote payments/e-commerce) are growing at unprecedented rates, consumers, issuers, and merchants have not abandoned physical payment options. To the contrary, physical payment transactions continue to grow and evolve. EMV has been implemented in the United States, as it has in other countries, with the goal of reducing card-present fraud. The recent EMV implementation focus has been centered on contactless form factors, which include (but are not limited to) contactless cards, Near Field Communication (NFC) enabled mobile devices, and wearables.

EMV contactless cards, mobile devices, and wearables interact with EMV-enabled POS devices in a standard EMV processing mode. While many similarities exist between contactless cards, mobile devices and wearables, several key differences remain. These differences include:

- The EMV card personalization process vs. the credential provisioning process to the mobile device or wearable
- The card primary account number (PAN) vs. the mobile device or wearable token[1]
- Lifecycle management of a card vs. lifecycle management of the credential
- The identifier for the credential container (once the credential is provisioned within the mobile device or wearable), also described as a wallet identifier

This white paper focuses on card-present transactions, with the following goals:

- Document three specific emerging data elements and how each is supported by the global payment networks today.
- Document use cases in which access, or earlier or broader access, to these three emerging data elements may benefit certain stakeholder groups.
- Provide recommendations regarding access to these three emerging data elements in connection with the identified use cases

The specific emerging data elements discussed in this paper include: token requestor identifier (TRID), wallet identifier (Wallet ID or WID), and Payment Account Reference (PAR). The white paper focuses on access to these emerging data elements for contactless face-to-face transactions.

[1] Additional information on tokenization can be found in the U.S. Payment Forum publication, "EMV Payment Tokenization Primer and Lessons Learned," June 2019.

2. Current Support for Emerging Data Elements

Currently, global payment network support for emerging data elements varies. To understand the current market offerings, it is important to understand the definitions for, availability of, and use cases for the token requestor identifier (TRID), wallet identifier (WID), and Payment Account Reference (PAR) data elements. This section describes the availability of these data elements for each global payment network.

A TRID correlates to the party who requested the payment token from the token service provider (TSP). The TRID is represented by a unique 11-digit numeric value assigned by the TSP. In some cases, this is the wallet provider, but many times the token requestor is a different party (e.g., issuer, service provider). As can be seen in Table 1 and Table 2, the TRID is currently more available for use in payment processing than the WID.

A WID correlates to the wallet that holds the payment token and that is presented at the POS. At present, the WID is most consistently used to notify issuers of wallets requesting the provisioning of their cardholder's account.

The PAR is a unique identifier associated with a specific PAN and any future evolutions of that PAN, regardless of device; it is not associated with a cardholder. Use of the PAR correlates activity across transactions linked to a PAN, including all its affiliated tokens.[2]

At this point in the marketplace evolution, the WID and TRID may not be the same for a given wallet provider. The marketplace is starting to see the emergence of token requestors that are not also wallet providers.

TRID, WID and PAR data element implementation is emerging. The current availability of each is shown in the following tables. Consult the payment networks for updates since information may change.

Table 1. Payment Network Support for TRID

Token Requestor Identifier (TRID)	American Express	Discover	Mastercard	Visa
Provided to issuer for OR at provisioning	Yes	Yes	Yes	Yes
Provided OR available at authorization request	Issuer	Issuer	Issuer	Issuer
Provided OR available at authorization response	Acquirer / merchant	Acquirer / merchant	Acquirer/ merchant	Acquirer[3]
Location of TRID	Subfield 5 of Bit 60 in the 1100 authorization request and 1110 authorization response	Authorization ISO Field 106 DS61 Tag02	DE 48, SE 33, SF 6	Field 123.68 tag 03

[2] Additional information on PAR can be found in the EMVCo publications, "EMV® Payment Tokenisation Specification – Technical Framework," Sept. 8, 2017, "EMVCo White Paper on Payment Account Reference (PAR)," Sept. 2019, and Secure Technology Alliance white paper, "EMVCo Payment Account Reference (PAR): A Primer," April 2018.

[3] Merchants should work with their acquirers to understand the supported methods to receive that information.

Table 2. Payment Network Support for WID

Wallet Identifier (WID)	American Express	Discover	Mastercard	Visa
Provided to issuer for OR at provisioning	Yes	Yes	Yes	N/A
Provided OR available at authorization request	Issuer	N/A	Issuer	N/A
Provided OR available at authorization response	No	N/A	Acquirer/ merchant	N/A
Location of WID	Auth 1100 (DF34, SF3) or Token 1100 (DF60, SF9)	N/A	Refer to Mastercard documentation	N/A
Format of WID (numeric, alpha and length)	2 bytes, alphanumeric	Max 100 alpha / numeric; can't contain all zeros, spaces, or special characters	Refer to Mastercard documentation	N/A

Table 3. Payment Network Support for PAR

Payment Account Reference (PAR)	American Express	Discover	Mastercard	Visa
Provided to issuer for OR at provisioning	No	Provided for all card types enrolled for Discover token services; the issuers do not need to opt in.	Yes, if the issuer has ability to maintain lifecycle then the PAR is assigned; provided in the auth-orization request.	Yes
Provided OR available at authorization request	Provided to issuer	Provided to issuer; where included in the card personali-zation, available to merchant/ acquirer.	Provided to the issuer on all transactions associated with the given PAN, once an issuer enrolls in tokenization and maintains a life cycle management tool.	Available on all PAN and payment token transactions. Always provided to the issuer at authorization and the issuer may elect to receive.
Provided OR available at authorization response	Provided to merchant acquirer	Yes	Provided to the acquirer on all transactions associated with the given PAN, once an issuer maintains	Always provided to the acquirer in the authorization response. The acquirer must provide to the

Payment Account Reference (PAR)	American Express	Discover	Mastercard	Visa
			tokenization and a life cycle management tool.	merchant if requested.
Batch availability	API available	API available	API available to issuers to generate a PAR value	Available to issuer or acquirer to request
On-demand availability	API available	API available for issuer, acquirer, merchant, and token requestor	API available for acquirer and issuer look-up	API available for issuer, acquirer, merchant, and token requestor
Location of PAR for EMV form factors (contact, contactless or mobile)	Field 55 (9F24) Available in specifications	Field 55 Tag 9F24 Authorization response (issuer): F56 (returned unchanged if provided by Discover in authorization request); populated with PAR (if non-token – when available)	Field 55 9F24	Field 55 9F24
Location of PAR within the authorization request and response	Field 112, subfield 1	Field 56 in authorization requests and responses[4]	Field 56 in authorization requests and responses	Field 56 in authorization requests and responses

[4] This is only for Discover – not for PULSE or Diners Club.

3. Use Cases / Scenarios

Access, or earlier or broader access, to TRID, WID or PAR may benefit certain stakeholder groups in a number of scenarios or use cases. This section describes some common scenarios in which such access may be particularly useful. While this paper's scope is primarily focused on contactless form factors, some use cases are relevant to both in-store and e-commerce environments. For all use cases described in this section where the WID or TRID may be helpful, the name/descriptor affiliated with the TRID or WID is also needed to ensure the data is understood and used appropriately.

3.1 Co-Marketing Opportunities

Co-marketing and loyalty opportunities with wallet providers and others are expected to drive use of mobile wallets. Co-marketing or loyalty messaging and offers are typically presented at the POS. In this scenario, merchants may choose to provide customers with offers or promotions at the POS based on the wallet being presented and certain other criteria (such as time of day, purchase amount or other criteria); the offer may be in the form of a product offering (e.g., free ice cream cone if you buy $10 with a certain wallet). If a co-marketing promotion depends on the wallet provider and changes the purchase price or identifies real-time bonuses the customer should receive for meeting the eligibility requirements of the co-marketing promotion, then the WID is required before the transaction is authorized. If the co-marketing promotion provides benefits outside of the POS interaction, the WID could be communicated at a later point in the transaction.

> **Relevant emerging data elements**: As this use case is specific to WID, the WID would best meet this scenario's requirements. To the extent that the TRID and WID are the same for a given wallet, the TRID could also be used. However, no payment networks currently have a WID or TRID available at the time the merchant creates the authorization request; this limits the ability for merchants to apply promotions based on the wallet provider at the POS. For wallets where the wallet provider is also the token requester, this value can be delivered outside of the POS experience.

3.2 Troubleshooting

The entire payments ecosystem, including cardholders, benefit from the ability to identify and resolve issues faster. The availability of transaction information, like the TRID and WID, may be important for mobile transaction troubleshooting where a wallet has been used. Issues that could potentially be resolved more easily where a wallet was used include, but are not limited to: failure to communicate payment information when requested; high decline or chargeback rates due to data quality issues; or other latency, process or operational issues. Once diagnosed, the merchant or other identifying stakeholder can proactively work with the wallet providers and other payment partners to resolve the issue. One example of an observed issue where a WID would have been useful is when consumers experienced declines with a specific issuer's cards (payment credentials) in a specific wallet at a merchant's POS. Another foreseeable scenario would be to identify where a wallet fails a required processing element for a transit payment transaction (e.g., because the wallet provisioning lacks offline data authentication (ODA) capability).

> **Relevant emerging data elements**: Both the TRID and WID may be beneficial for troubleshooting certain issues. If TRID and WID are the same for a given wallet, access to either may be useful. Making these data elements available earlier in the process may expand their usefulness in troubleshooting.

3.3 Customer Service, Returns and Disputes

One complexity created by the use of tokens is that the last four digits of the payment credential is different from the last four digits of the cardholder's credit or debit card number. This may cause confusion for customers when discussing transactions with an issuer or merchant service representative, or when initiating a return or dispute. Availability of WID may help to reduce this confusion by enabling the representative to share that the transaction in question, or the one associated with the return, was completed with a specific wallet, and that this is why the last four numbers are different.

The PAR can also be used in the receipt look-up process to identify the original purchase transaction, even when the purchase and return took place in different channels or with different form factors of the same PAN. PAR may also be helpful for cross-device account identification in transit.

> **Relevant emerging data elements**: For customer service inquiries, including disputes, the WID would be helpful, as the representative could identify and share the specific wallet used. However, the TRID would also be helpful to identify that the transaction was completed with a wallet. Because the customer interaction involved in these scenarios takes place after the original transaction at POS, the data elements are useful if received in the authorization response.
>
> For returns, the PAR is most beneficial when available at the time of the return presentment. With PAR, the merchant can ensure the return is associated with the PAN that was used in the original transaction, even if the token and card number differ. For transit, PAR can be leveraged from the authorization response, but may also be useful if transmitted in the contactless tap.

3.4 Analytics

Leveraging emerging data elements in analysis can assist companies in understanding customer shopping preferences, in improving business practices, and in managing compliance.

Awareness of customer preferences is critical to meeting their needs. For example, analysis of wallet usage at a merchant can help it best tailor wallet partnerships (i.e., co-marketing) to better serve their customers. Once implemented, leveraging wallet information in activity analysis can validate whether the success metrics for the partnership have been achieved. In addition, PAR can be used to analyze engagement and loyalty, such as customer overall spend or number of trips. This analysis could be further delineated by wallet if a WID was included in the analysis.

In addition to usage trends, analytics are used to improve business processes, manage operations and control expense. Correlation between wallet usage and preferred servicing engagement methods can advise future customer service alignment, and analysis of chargeback rates by wallet can provide valuable insight to improve operations. Many other analyses would benefit from wallet information, but the availability of a method to identify a wallet is required to enable these.

Finally, emerging data elements can be used in analytics to support compliance programs. One example is the PAR, which can be used to correlate transactions for anti-money laundering (AML) monitoring and other compliance reporting.

> **Relevant emerging data elements**: Relative to TRID, the WID provides the greatest amount of detail for the transaction, so can be the most valuable analytically. The TRID can also be useful, but provides less granularity and usage information than the WID. As analysis is conducted after the POS transaction, the data elements can be received in the authorization response or any time after for the analysis use case.

PAR supports different analytical approaches and compliance programs. For most analytical purposes, it may be sufficient to receive PAR in the authorization response; however, for some use cases, like real-time compliance monitoring, receiving the PAR with the payment credentials at the time of the transaction may be needed.

3.5 Improved Support of Unique Features and Financial Models

New and emerging wallet providers may operate with different transaction features and under various settlement procedures and timing. The availability of a WID can help merchants to provide an appropriate transaction experience for the customer and can enable merchants to better project cash flows to reduce settlement risk for these wallet providers.

Relevant emerging data elements: The WID can be most valuable for this use case. The TRID would be helpful to the extent that the wallet provider is also the token requester. As settlement balancing is conducted following the transaction, the data elements can be received in the authorization response for this use case.

3.6 Improved Authorizations and Better Fraud Prevention

Particularly in the e-commerce environment, additional data can lead to improved authorization rates and more effective fraud prevention. Merchants, issuers, and payment networks all have an interest in improving authorizations and reducing false positives.

Merchants often use layered tools and technologies to prevent fraud. These generally leverage key transactional data such as device ID, geolocation, and known customer purchasing behaviors across channels. The introduction of tokenization and wallets added complexity to fraud prevention and authorization optimization, as merchants may not have full transparency to newly relevant transactional data. For example, a single fraudster could transact across e-commerce and in-store channels or with multiple devices – all with different tokens and the original PAN – and the merchant could have no way to know it was the same person. The same is true in the e-commerce space, where there may not be a correlation between a card number entered on a website and the same card presented as a token in a wallet in-app or web-based transaction.

Merchants could also leverage wallet data in their authorization and fraud routines. This provides a deeper data set upon which to build strategies, and could promote less friction in the checkout process. For example, a merchant may identify a trusted third-party wallet when presented at the point of customer interaction and execute a more streamlined checkout flow reflective of the perceived transaction risk.

Relevant emerging data elements: To tie customer transactions for fraud prevention purposes, PAR can be most relevant as it correlates the original PAN and any affiliated tokens. Receiving PAR in the authorization response can suit some needs, but the introduction of PAR at the payment capture could enable the affiliation of unrecognized, newly presented tokens with previously-processed transactions with the same correlated PAN. This early correlation can lead to a better authorization and fraud prevention decisions.

The WID expands on the utility of PAR for this use case, bringing deeper information about the payment's origination. This information can be useful in the authorization response for fraud and authorization decisioning, but could be optimal at the time of transaction to reduce friction in the checkout process. To the extent that the TRID and WID are the same for a given wallet, the TRID could be used for that wallet.

4. Recommendations to Address Use Cases

In reviewing the use cases in Section 3 and the options to address each, two sets of variables emerge. The first is specific to the WID and TRID — the granularity of the data needed to address the use case. The second is when the data is available and applies to WID, TRID and PAR. The WID, TRID and PAR could be provided in reporting, in provisioning, before the authorization request, or in the authorization response. When the data is available impacts the utility of the data element for each use case. In all cases, the data availability consistency is critical, so the data can be relied upon to meet the use case needs.

For wallet identification, where WID and TRID are options to address use cases in Section 3, generally, WID information in transaction processing would be most valuable. However, a spectrum of data and timing combinations can provide varying levels of support for use case requirements. For example, for troubleshooting, customer service, and analytics, more granular information, earlier in the process, is generally better. While this may indicate that WID would be more helpful for these use cases, much can be learned from the TRID and used for these use cases. Basic analysis of TRID usage trends may indicate new wallets in the market and shifts in consumer preferences. This analysis provides a baseline understanding; however, the more granular WID may be useful as the digital market expands. In troubleshooting, TRID can be used to solve certain issues or to identify the appropriate parties with whom to work to identify solutions. For these use cases, making the TRID, and the related TRID description, available to all stakeholders would be valuable. Troubleshooting more complex issues may need data that is specific to the wallet, such as WID.

PAR use cases are emerging. For the use cases identified in Section 3 (e.g., receipt lookup for returns and compliance programs), early availability of the PAR, ideally before the authorization request, is preferred. For other analytical uses of PAR, receiving this data in the authorization response or in a batch process may be sufficient.

For other use cases, such as co-marketing, loyalty, and leveraging data to improve authorization rates and better fight fraud, TRID is helpful to the extent that the wallet provider is also the token requestor. At this phase in the U.S. implementation of digital payments, this combination may be found more frequently than one might expect as the market expands and the number of wallet providers or token requestors increases. PAR can also be helpful in promoting improved authorization rates and reduced fraud by creating transparency to prior purchase history with the same PAN through other tokens or the PAN itself. This is especially important as cardholders shop across channels.

Given the variation in the granularity and time of availability of these emerging data elements a progressive path may be helpful to meet the use cases noted in Section 3. Figure 1 illustrates one possible implementation sequence to broaden the availability of WID, TRID, and PAR, and to consider the timing needed for the use cases. Because TRID is currently used in payment processing for all payment networks identified in Section 1 and is available to many payment stakeholders, expanding TRID availability provides the foundation to begin to address the use cases for all stakeholders.

Figure 1. *Potential* Timing and Process for Providing TRID, WID and PAR for Payment Processing

1. Provide reporting of transactions based on TRID (and TRID descriptor) to interested stakeholders including merchants.
2. To the extent provided to the acquirer, provide TRID and PAR to merchants in the authorization response.
3. Include PAR data in the EMV payment token[5] provisioning data (wallet, card on file and issuers).
4. Enable the ability for merchants and other stakeholders to perform a PAR inquiry for tokenized and PAN transactions (to the extent that a token has been provisioned for a PAN or a PAR is available for the PAN).
5. Provide TRID and PAR to merchants for, or prior to, the authorization request.
6. Provide reporting of transactions based on WID (and WID descriptor) to interested stakeholders including merchants.
7. Include PAR data in the EMV chip data for contact and contactless cards (clear text account numbers).
8. Provide WID to issuers during the provisioning process.
9. Provide WID to merchants, issuers, and other relevant stakeholders in transaction processing. Share with issuers in the authorization request and with merchants in the authorization response.
10. Provide WID to merchants, issuers, and other relevant stakeholders in transaction processing. Share with merchants prior to the authorization request, and to issuers with authorization request.

[5] 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.

5. Conclusion

The U.S. Payments Forum developed this white paper to provide an educational resource for merchants and the payment acceptance community, as a result of increased interest and opportunity in device-centric, face-to-face payments. As device-centric digital payments expand in the U.S., understanding the data elements that are available to link the payment credential and device to the customer for loyalty or other use cases is top of mind for merchants.

The information presented in this white paper is intended to provide an overview of the emerging data elements available to the payments ecosystem for face-to-face transactions initiated from non-traditional payment devices. Merchants, payment gateways, and acquirers should consult their payment networks or payment partners for additional details on enabling these data elements to support these use cases.

6. Supplemental Definitions

Term	Related terms	Definition	Source
Digital Wallet	eWallet	A software representation of a physical wallet. For example, putting debit and credit cards into an application that holds payment credentials through which someone can pay, using the digital version of the debit or credit cards in that person's physical wallet, linking to the same account, to pay.	U.S. Payments Forum
Mobile Payment Device		This term can be both broadly and specifically defined. The broad use could be a device that supports payment, including wearables, both with passive power or battery-powered sources. Specifically, most common examples include smartphones and tablets.	U.S. Payments Forum
Mobile Wallet		The mobile version of a digital wallet, provisioned and accessed on a mobile device.	U.S. Payments Forum
NFC	Near Field Communication ISO 18092	NFC is a set of standards that enables proximity-based communication between consumer electronic devices such as mobile phones, tablets, personal computers or wearable devices. An NFC-enabled mobile device can communicate with a POS system that currently accepts contactless payment cards.	U.S. Payments Forum
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.	EMVCo
Primary Account Number		A variable length, ISO/IEC 7812-compliant account number that is generated within account ranges associated with a BIN by a card issuer.	EMVCo
Payment Account Reference		A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated payment token.	EMVCo
Provisioning		An initial set up process that handles authentication of a user account, the exchange of keys to unlock the NFC chip installed on a mobile device, the service activation and the secure download of mobile payment account information.	U.S. Payments Forum
Token Requestor		Entity that initiates requests that PANs be replaced with non-sensitive tokens for long-term storage and future use by submitting token requests to the token service provider.	U.S. Payments Forum

Term	Related terms	Definition	Source
Token Requestor ID		An 11-digit numeric value that identifies each unique combination of token requestor and token domain(s) for a given token service provider.	EMVCo
Wallet Identifier		The container in which the payment credential is provisioned, which is initiating and being responded to via a transaction at a POS. The identification of this container has been described as a wallet identifier.	U.S. Payments Forum Mobile and Contactless Payments Working Committee
Wallet Service Provider		Companies that offer specific wallet solutions that use various communications technology for mobile payments.	U.S. Payments Forum

7. Legal Notice

The U.S. Payments Forum endeavors to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. This document is intended solely for the convenience of its readers, does not constitute legal advice, and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including but not limited to warranties regarding the accuracy, completeness or adequacy of information herein. Merchants, issuers and others considering implementing contactless technology are strongly encouraged to consult with the relevant payment networks, vendors and other stakeholders prior to implementation.