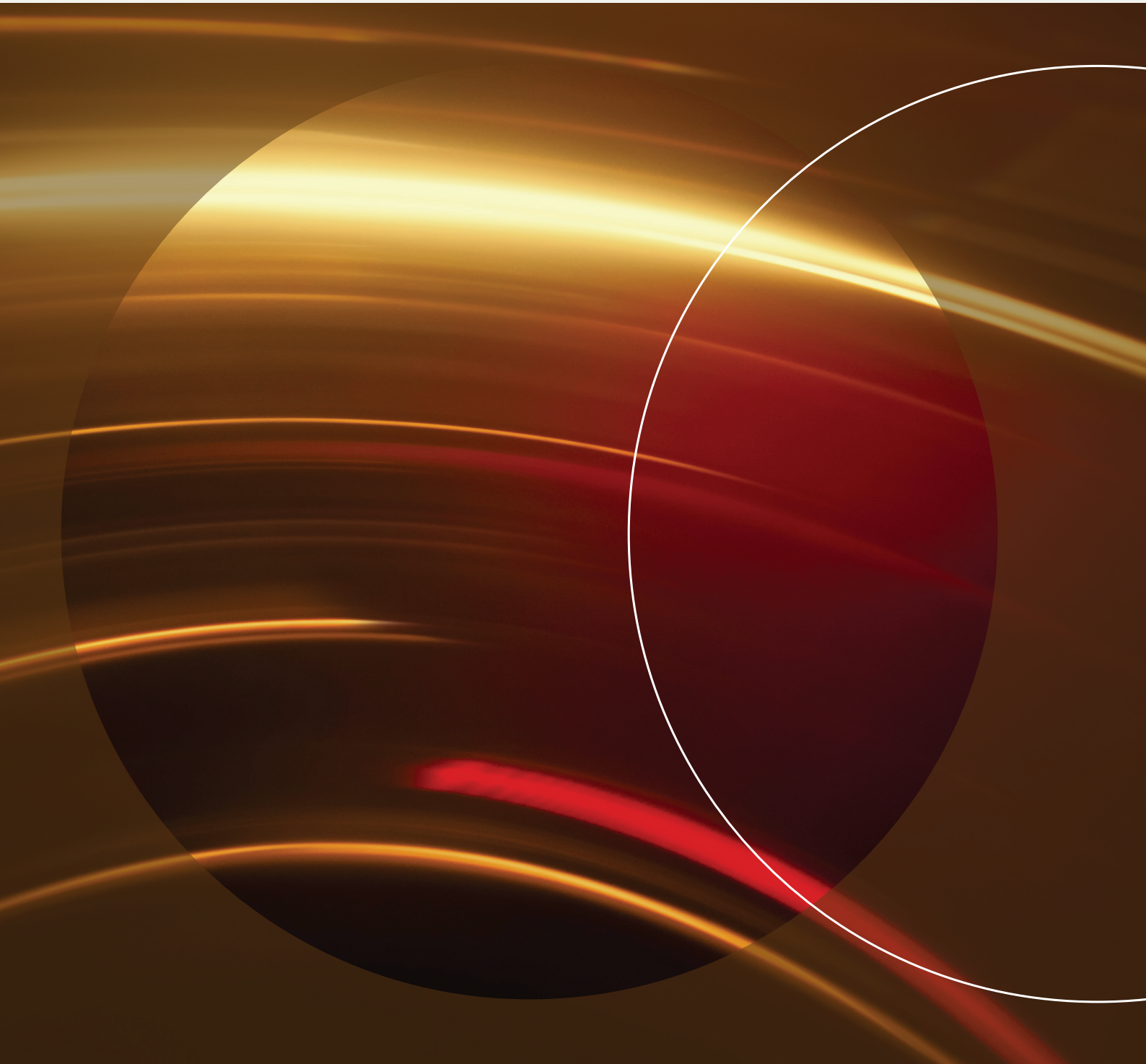
WHITE PAPER
DECEMBER 2025

Mastercard Digital Payment Security Standard

The gold standard for online payments



Contents

Supporting the future of e-commerce with Digital Payment Security Standard

$15b

Total cost of third-party CNP fraud[2]

"Digital Payment Security Standard — a blueprint for secure, high-quality transactions.

Global e-commerce payments are projected to surpass $7.9 trillion by 2028 — but only if there is trust in the payments ecosystem.[1]

E-commerce continues to evolve rapidly with new use cases, such as agentic payments and in-car commerce, pointing toward an exciting future for online transactions. But to fully realize this potential, the underlying technologies that secure these transactions must be strengthened, especially as third party card-not-present (CNP) fraud continues to adapt and become increasingly sophisticated. CNP fraud is estimated to cost $15 billion annually.[2] The traditional e-commerce safeguards of passwords and one-time passcodes (OTPs) have fallen short in addressing the security challenges these remote transactions pose for merchants and issuers. Realizing this, Mastercard has been actively working to strengthen and future-proof online payment experiences.

To help navigate these complexities, Mastercard is introducing Digital Payment Security Standard (DPSS), a framework that establishes the key principles of good, high-quality transactions. This framework promotes the optimal approach for ensuring that online payments continue to grow while maximizing conversion, increasing approval rate and minimizing fraud. DPSS is built from best practices and regulation observed across the global e-commerce landscape, and is made up of three key pillars:

Verified Token: Tokenization secures online payments by replacing the card number with a unique token—protecting sensitive payment data. A Verified Token adds another layer of security as it is a token that is created after the cardholder's identity has been authenticated by the issuer. The combination of tokenization and authentication gives merchants and issuers confidence that a transaction is secure and initiated by the rightful cardholder.

Enhanced Data Sharing: When merchants share more insights and contextual data (such as cardholder, merchant, and device data), it powers the issuer's ability to more accurately assess a transaction and make an informed decision, resulting in improved cardholder experience, higher conversion, lower fraud, and better approval rates.

Seamless Authentication: Access to Enhanced Data enables low-risk transactions to be authenticated without a challenge, meaning no additional verification step is needed. For high-risk transactions that require a challenge, technologies like biometrics can help reduce friction at checkout.

Issuers, acquirers, merchants and other payments ecosystem stakeholders stand to benefit from following the practices outlined within DPSS. By enhancing security and data sharing, DPSS is designed to support better decision-making for issuers and create a smoother checkout experience for merchants and shoppers.

Introduction

↓3x

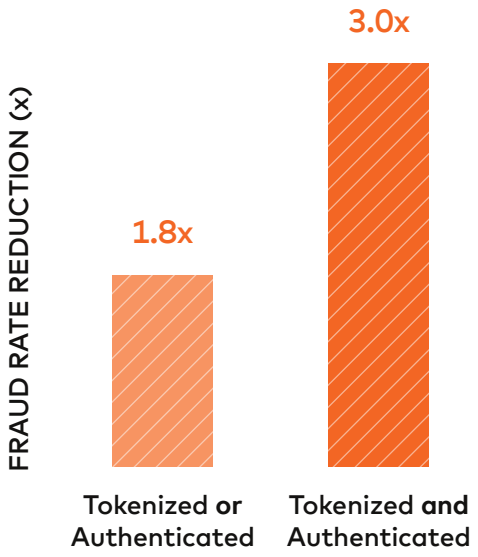
less fraud when transactions are tokenized and authenticated in the EU and the U.K.[4]

Online payments are driving the growth of numerous industries, and it is high time that related challenges are addressed to make these transactions even more secure. Current efforts to combat these issues have resulted in limited success, and more can be done. For example, forty-three percent of consumers gave up on a purchase in the previous 60 days because they forgot their passwords, and OTPs create a clunky and inconsistent experience, and potentially a prime phishing opportunity.[3]

High fraud, poor approval performance, and low conversion challenges have been accepted as the cost of doing business online, but they do not have to be. In the EU and U.K., when transactions are both tokenized and authenticated there is 3x less fraud than when neither tokenization or authentication are used, showcasing the incremental value of utilizing both.[4]

Tokenization adoption has boosted approval rates 3-6 percentage points globally.[5] Additionally, when biometrics are used in place of OTPs, there is 2.5x less fraud.[6] But despite clear signs of success, such solutions have not yet been applied consistently across the payments landscape due to different factors including the perceived cost of implementation, potential operational complexity, and concerns about affecting conversion. As a result, this has limited the impact of tokenization and authentication.

The combination of tokenization and authentication delivers the highest improvement in fraud



As compared to untokenized and unauthenticated transactions

Mastercard is committed to transforming online checkout to support the payments environment, maximizing conversion and minimizing fraud.

Regulations like Payment Services Directive 2 (PSD2) and specifications including Fast Identity Online (FIDO) standards have helped address some experience and security challenges facing online transactions, but more is needed to improve three key areas:

- **Consumer control:** Consumers often feel uneasy or insecure about sharing their credentials online and may be uncertain about the nature of their payments, such as an automatic payment made for a forgotten subscription. In fact, 58% of consumers do not feel comfortable entering financial data online to make a purchase.[7]
- **Data sharing:** When merchants are unable to provide sufficient insights and high quality data to issuers, it can lead to issuer declines resulting in checkout friction.
- **Better authentication:** If issuers do not implement simple and secure authentication methods, it can lead to unnecessary friction that can frustrate consumers, and may cause abandonment.

Mastercard aims to address these areas in a few ways. First, Mastercard is targeting 2030 to eliminate the need for manual card entry and one-time or static passwords by combining tokenization with authentication to enable a more secure, seamless checkout.

Second, the three pillars of DPSS - Verified Token, Enhanced Data Sharing, and Seamless Authentication - are designed to address these challenges and support improvements in online payments for stakeholders across the ecosystem.

By the end of the decade, Mastercard aims to phase out manual card and password entry in favor of smiles and fingerprints globally, paving the way for a future where numberless cards are the default.

A new standard built on three pillars

Digital Payment Security Standard (DPSS) is a framework that outlines the vision for a gold standard transaction based on tokenization, data sharing and authentication.

The framework secures digital payments for consumer-initiated transactions (CITs) and merchant-initiated transactions (MITs). By adhering to its principles, issuing and acceptance partners will benefit from reduced fraud, improved approval rates and higher conversion. Additionally, when stakeholders follow the DPSS framework, they will deepen consumer trust and further the growth of their online businesses.

DPSS is built on three pillars: Verified Token, Enhanced Data Sharing, and Seamless Authentication. The use of a Verified Token, a token with cardholder identity verification, enhances consumer trust in online payments and gives issuers greater assurance that the transaction is authorized by the legitimate cardholder. Enhanced Data Sharing improves data exchanges between merchants and issuers which facilitates better decisions, while Seamless Authentication leads to less friction in the overall payment experience.

Verified Token

Utilize Verified Tokens as payment credentials

Bind payment credentials to the consumer's device

Enhanced Data Sharing

Implement intent management for tokenized transactions

Generate a unique identifier for CITs

Employ contextual data to aid decisioning

Leverage transaction-unique dynamic data for transactions

Seamless Authentication

Use risk assessment data

Utilize cardholder authentication with CITs

Apply biometric authentication for optimal performance with challenged transactions

Verified Token

↑ 2%

incremental approval rate from a Verified Token vs. a Token.[8]

Enhancing tokens with Verified Tokens is at the heart of the effort to improve CNP transaction performance. Arming merchants and issuers with the knowledge that each transaction is tokenized and comes from an authenticated cardholder, allows them to fully harness the combined security of tokenization and authentication. Additionally, this pillar tackles the issue of consumers' insecurity about sharing their credentials through identity verification.

The Verified Token pillar is underpinned by two principles and serves as a vital cornerstone of DPSS:

- **Utilize Verified Tokens as payment credentials:** Verified Tokens, created after the cardholder's identity has been authenticated by the issuer, are used to enhance the security of card-on-file and card-based alternative payment methods (e.g., digital wallet payments) transactions.
- **Bind payment credentials to the consumer's device:** Credentials are bound to the consumer's device to establish a verified possession factor for CITs.

Enhanced Data Sharing

↓ 40%

An external party's data sharing program showed a reduction in false positives declines.[9]

The Enhanced Data Sharing pillar has proven to reduce fraud and increase approval rates. This is demonstrated by an external party's data sharing program, which generated a 40% reduction in false positives declines.[9] When merchants share more insights and contextual data, it powers the issuer's ability to better assess a transaction and make an informed decision. As a result, issuers and merchant can avoid unnecessary authentication challenges given issuers' increased confidence in the transaction. This improves the cardholder's experience and improves conversions.

The Enhanced Data Sharing pillar is underpinned by four principles, driving trust in the ecosystem:

- **Implement intent management for tokenized transactions:** Intent management ensures that a cardholder's stated intent to pay — reflected in payment details such as merchant name and transaction amount — is clearly understood and validated, enabling more accurate decisions and lowering risk across the payment flow. Intent management applies to various CITs including CITs associated with subscriptions.
- **Generate a unique identifier for CITs:** CITs contain a unique identifier (e.g., Trace ID) sent in authorization to the issuer, that can be utilized with recurring payments to associate a CIT with an MIT, supporting higher approvals.
- **Employ contextual data to aid decisioning:** Additional contextual data (such as cardholder, intent payment details, and device) is shared with the issuer to improve decisioning.
- **Leverage transaction-unique dynamic data for transactions:** The cryptogram binds the transaction details and token, adding an additional layer of security by ensuring the integrity of the payment data.

Seamless Authentication

55%

of consumers would abandon a purchase mid-way through due to friction.[10]

The Seamless Authentication pillar is centered on streamlining authentication to improve decisioning and security, without sacrificing the user experience. It is critical that simple and secure authentication processes are used because 55% of consumers have indicated that they would abandon a purchase midway through due to friction.[10] Notably, authentication should not be synonymous with a challenge. Instead, authentication should be optimized based on the riskiness of a transaction. For a low-risk transaction, a challenge is not needed. For a high-risk transaction, a challenge is required and should rely on a secure, seamless multi-factor authentication (MFA) method such as biometric.*

The Seamless Authentication pillar is based on three principles that are designed to support each transaction with an authentication method appropriate to its risk level:

- **Use of risk assessment data:** Risk-based decisioning leverages risk assessment data (e.g., scores, reason codes) and is a dynamic, intelligent security layer used by ecosystem stakeholders to not only assess transaction riskiness but also determine the best authentication method.
- **Utilize cardholder authentication with CITs:** An issuer-agreed authentication method based on risk level should be used for CIT transactions.
- **Apply biometric authentication for optimal performance with challenged transactions:** Employ biometric authentication to reduce fraud risk on CNP transactions as it uses the cardholder's unique characteristic for validation.

An example of a frictionless authentication on a transaction identified as low-risk using data sharing

How it works:

- Merchant shares a Verified Token and Enhanced Data with the issuer.
- Issuer uses this data in risk modeling to assess transaction risk.

If low-risk is confirmed:

- No step-up authentication is required.
- Frictionless checkout experience for the customer.

Key benefits:

- Merchants reduce cart abandonment, resulting in higher conversions.
- Issuers gain higher approval rates and reduced fraud. No fraud liability shift involved.

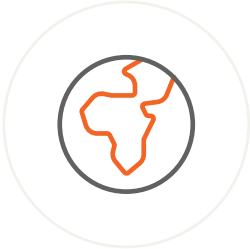
*Subject to local regulations

A win for both sides: benefits for issuing and acceptance partners

Digital Payment Security Standard helps issuers and merchants boost e-commerce success by optimizing online performance.

It arms issuers with more data, enabling them to make more confident decisions, lower fraud and boost approval rates. For merchants, DPSS reduces check out friction by minimizing unnecessary challenges while ensuring the right transactions are examined more closely.

Two examples of what Digital Payment Security Standard can look like in action:



Consumers often make everyday purchases online, such as meal delivery, pet supplies and music. Enhanced Data Sharing facilitates the issuers' ability to eliminate unnecessary friction for these low-risk transactions given their alignment with the cardholder's established behavior.

Specifically, when a cardholder initiates such an everyday transaction, the issuer's risk assessment confirms that the spending pattern matches historical norms and shows no indication of fraud. As a result, the transaction qualifies as low-risk and is processed through frictionless authentication, with no challenge required. This allows the payment to be completed smoothly and without interruption, not only increasing issuer approval and merchant conversion but also cardholder satisfaction.

Online transactions are growing to include new types of payments like agentic commerce and in-car commerce. These and other future use cases hold tremendous potential for ecosystem growth, but they will benefit from a consistent framework to keep conversion and approvals high.

Intent management is particularly critical with the emergence of agentic payments, in which an AI agent makes a purchase on behalf of a cardholder. Intent management ensures that the cardholder's stated intention to pay as captured by payment details (e.g., merchant name, purchase amount) is authorized and accurate. This enables a smoother consumer experience while minimizing the potential for disputes and chargebacks.

Future ready, today.

Mastercard is powering the future of digital commerce with Digital Payment Security Standard, laying the groundwork for a smarter, safer and more seamless cardholder experience.

As e-commerce accelerates, we're not just adapting—we're leading. DPSS is designed to tackle today's toughest challenges in fraud prevention, approval optimization, and conversion performance. It's also built to meet the evolving expectations of today's digitally savvy shoppers—and tomorrow's. Throughout 2026, we will launch new solutions, enhancements and rules to support DPSS.

In a world where trust and transparency will be more paramount than ever, we're setting the pace for a faster, safer, and more resilient digital commerce ecosystem—together with our partners.

For more information contact your Mastercard account representative

1. Worldwide Retail Ecommerce Forecast 2025, April 2025, https://www.emarketer.com/content/worldwide-retail-ecommerce-forecast-2025
2. Boston Consulting Group Authentication Market Study, North America, Jan 2025
3. "FIDO Alliance study reveals growing demand for password alternatives as AI-fueled phishing attacks rise, " Oct 2023, www.fidoalliance.org
4. Mastercard internal data.
5. Mastercard internal data. Benchmarked 2024 sample of MDES for Merchants customers on CNP first attempt transactions. Varies by region.
6. Mastercard internal data, 2024
7. Business Wire "Consumers' Online Payment Security Fears Grow Following 'Cost-of-Living Crisis', Says Paysafe Research," Sept 2022
8. Mastercard internal data.
9. Wheeler, Kitty "How Worldpay & Capital One Tech is Combating Payment Fraud" Cyber Magazine, Oct 2024.
10. PYMNTS.com "Online retailers lose half of sales to checkout friction," Jan 2023

Detailed breakdown of the principles of each pillar of DPSS

Verified Token

UTILIZE VERIFIED TOKENS AS PAYMENT CREDENTIALS

Verified Tokens are used to secure tokenized transactions. Verified Tokens are established once the identity of the cardholder has been verified using an authentication method, typically provided by the issuer.

Tokens provide significant benefits in transaction processing compared to FPANs, including the enforcement of token domain controls as a token can be restricted for use under agreed conditions, such as limiting it for use by a specific merchant or for e-commerce transactions. A token can also be suspended from use without affecting other tokens of the same FPAN, or the FPAN itself.

BIND PAYMENT CREDENTIALS TO THE CONSUMER'S DEVICE

Payment credentials are bound to the consumer's device to establish a verified possession factor for CITs. These device bindings are established after verifying the identity of the cardholder on the device using an MFA method typically provided by the issuer. The resulting binding ID is an identifier bound to the consumer device that is shared with the issuer and can be used to recognize consumer devices during subsequent checkouts and transaction processing.

Mastercard performs device binding validations during checkout processing when MFA methods are utilized under Mastercard's Token Authentication Framework (TAF)**. The issuer receives the device binding ID from the Mastercard network during authorization processing and can perform further validation checks.

Enhanced Data Sharing

IMPLEMENT INTENT MANAGEMENT FOR TOKENIZED TRANSACTIONS

To ensure the quality of tokenized transactions, it is essential that cardholders are provided with clear transaction information (e.g., merchant name and purchase amount) along with transaction terms and conditions (e.g., payment frequency and amount of future related MITs for subscriptions).

Intent management captures the intent to pay, conveyed by the payment details of the transaction, and is accurately interpreted and confirmed, supporting better authorization decisions and reducing overall payment risk.

***More information about Token Authentication Framework can be found on Mastercard Connect.*

As identified previously, intent management applies to various CITs including CITs associated with subscriptions. Therefore, merchants may be obligated to perform cardholder authentication, in line with regulatory requirements, when the terms of the original intent changes (e.g., new price) as it alters the MIT details.

Proper intent management not only facilitates more accurate transaction assessment but also reduces disputes as the intent confirms that the transaction is authorized and understood by the cardholder.

GENERATE A UNIQUE IDENTIFIER FOR CITS

For CITs, a unique identifier (e.g., Trace ID) is generated by the Mastercard network and sent to the acquirer. For any subsequent MITs, the acquirer should send the unique identifier of the CIT in authorization to the issuer, so the transactions can be linked. The linkage creates an association between a CIT and MIT and thereby, assisting the issuer in making informed authorization decisions and avoiding unnecessary chargebacks.

When the unique identifier is combined with intent management, it allows for even better transparency. Specifically, the unique identifier can be leveraged to correlate CIT payment details captured by intent management with subsequent MITs. Mastercard uses the intent data to generate and share insights with the issuer on MITs to improve risk modelling and increase approvals. The process goes as follows:

- A standardized identifier is generated for a CIT and is referenced in the subsequent MIT.
- The payment details (e.g., merchant name, purchase amount, frequency of payment) captured by intent management is shared with the issuer. The unique identifier is leveraged to link the CIT with subsequent MITs.
- Strong Customer Authentication (SCA) on CITs is governed by regulations in some markets and is optional but recommended in other markets.
- Notification to the consumer of upcoming recurring payments may be required in regulated regions or under certain conditions as required by Mastercard rules. The issuer or the merchant will notify the consumer about the upcoming payment. A new cryptogram may be produced for the MIT. The issuer may request the consumer to re-authenticate the MIT as required.

EMPLOY CONTEXTUAL DATA TO AID DECISIONING

Data sharing between merchant and issuer ensures data is leveraged by risk models to reduce challenge-based authentication, minimize false declines and lower fraud. Contextual data include both standard data (information needed to process a transaction) and enhanced data (information not necessarily needed to process a transaction but can be used to augment modeling):

Standard Data

- Transaction data: Account number, purchase amount, purchase currency, purchase date, etc.
- Device data: Device channel, 3RI indicator, message category, message type, etc.
- Merchant data: Merchant name, merchant category code, acquirer merchant ID, etc.
- Token data: Token history, account tenure, wallet provide scores, etc.

Enhanced Data

- Cardholder data: Cardholder name, phone number, email address, shipping address, and billing address
- Device data: Consumer device name, consumer device location, consumer device ID/binding, and IP address
- Intent payment data: Examples include merchant name, account number, purchase amount, first and last transaction date, fixed/variable payment indicator and frequency of payment
- Merchant transaction assessment score: Transaction riskiness evaluation which may include merchant's transaction risk score or Mastercard's Merchant Trust Assessment signal

Mastercard's network facilitates the sharing of detailed transaction data, including Identity and Verification (ID&V) and authentication data, between the merchant/PSP and the issuer. Mastercard monitors and augments this data to ensure its accuracy, completeness and integrity.

LEVERAGE TRANSACTION-UNIQUE DYNAMIC DATA FOR TRANSACTIONS

This requires generating and validating a cryptogram which binds transaction details to the token. The cryptogram supports dynamic linking of the acceptor name and the transaction amount, the enforcement of token domain controls, and the confirmation that cardholder authentication occurred at the time of the original CIT. This enables greater confirmation of transaction authentication and can combat potential fraud.

Seamless Authentication

USE RISK ASSESSMENT DATA

Risk-based decisioning is a dynamic and intelligence based security layer that helps CNP transaction participants determine the riskiness of the transaction, helping with the choice of the best authentication path for the consumer.

The risk assessment data, which is generated by the networks, include network data, historical payment behavior, historical risk scores, authentication approvals, authorization history, token history, chargeback data and risk-signals (e.g., identity risk, IP risk, and compromised account numbers).

The machine learning (ML)/artificial intelligence (AI) decision model includes features like identity velocities, merchant velocities, environment velocities, pairs, continuous learning, regional models and routine fraud snapshots.

A holistic risk score is shared across to all ecosystem participants, including issuers, acquirers, merchants, and 3rd party operators, with reason codes for explainability and single-input category signals (e.g., an email risk score).

Merchants and payment service providers (PSPs) can share their insights on consumers based on their assessment, consumer purchase history and location, and the issuers can use that for improved decisioning during authorization.

UTILIZE CARDHOLDER AUTHENTICATION WITH CITS

An issuer-agreed authentication method is used for CITs when required by program rules, applicable regulation, and/or needed to obtain dispute liability protection per the standards.

The authentication can be a challenge-less risk based authentication method for transactions that are scored as low-risk (aligned with applicable regulation). For high-risk transactions, a challenge-based authentication must be used. The challenge-based authentication must be an MFA method.

An MFA is used to verify the identity of the cardholder for transactions. Authentication methods include issuer methods (such as 3DS Payment Authentication), or TAF methods (such as Mastercard payment passkeys).

For transaction amounts exceeding a region specific or country specific threshold for FPAN and Verified Token Transactions, the merchant or other acceptor may initiate an issuer-approved, challenge-based MFA method of the cardholder.

APPLY BIOMETRIC AUTHENTICATION FOR OPTIMAL PERFORMANCE WITH CHALLENGED TRANSACTIONS

Biometric authentication offers a secure and user friendly approach for handling challenged transactions by verifying a customer's identity through inherent physical traits—such as fingerprints, facial recognition, or voice patterns—rather than knowledge based credentials that can be forgotten, stolen, or intercepted.

Integrating biometrics into step-up or high-risk transaction flows significantly reduces fraud exposure by ensuring that only the legitimate cardholder can complete a transaction.

At the same time, it streamlines the customer experience by enabling fast, seamless verification without relying on cumbersome passwords or one time codes. This combination of stronger security, improved usability, and reduced friction provides substantial value by balancing risk management with customer convenience.

This document is proprietary to Mastercard and shall not be disclosed or passed on to any person or be reproduced, copied, distributed, referenced, disclosed, or published in whole or in part without the prior written consent of Mastercard. Any estimates, projections, and information contained herein have been obtained from public sources or are based upon estimates and projections and involve numerous and significant subjective determinations, and there is no assurance that such estimates and projections will be realized. No representation or warranty, express or implied, is made as to the accuracy and completeness of such information, and nothing contained herein is or shall be relied upon as a representation, whether as to the past, the present, or the future.