# Optimizing the Payment Authorization Rate

*Author: Mayank Taneja*
*Source: PaymentsJournal*
*Publication Date: March 18, 2024*

## Introduction

In the e-commerce space, a merchant's goal is to ensure exceptional ease and satisfaction during a customer's purchase lifecycle, which initiates with the first visit to the merchant's website and extends through the receipt of goods or services. From the merchant's perspective, the experience is complete when the seller has received payment in full, without any fraud or chargebacks.

Since payment is such a critical component of the customer's buying journey, merchants often have a dedicated payments product, engineering, and data science team to ensure that the last and most important step of the customer experience is smooth and rewarding. To facilitate positive payment experiences, the payment product team continually drives efforts to measure and improve various key payment metrics, including the authentication rate, the authorization rate, the chargeback rate, and the fraud rate. Almost all of these key payment metrics are intertwined to control fraud, while ensuring an optimal customer experience, to fulfill the objective of approving the highest possible number of good transactions.

## Why the Authorization Rate Matters

In the payments process, the user interface (UI) and user experience (UX) are significant for both the customer and business growth. However, providing the customer with a seamless payment process to complete the purchase is indispensable. An inability to get the payment authorized quickly would prevent the customer from completing the transaction. While this may be less impactful for a customer who has various payment and/or purchasing options, the merchant will invariably suffer from a loss of revenue, reputation, or potential customers—or in the worst case, all of the above.

Payment declines may happen during authorization because the issuer is flagging the transaction as fraudulent, but there are times when the declination may be triggered because the issuer's fraud machine learning (ML) models are erroneously identifying a non-fraud customer transaction as a fraud transaction. Hence, the merchant's payment platform product team must apply mechanisms to assure the internal ML's proficiency, so that they can better serve their customers by detecting bad transactions before they even hit the issuer's authorization processing stage. The merchant's transaction payload must also populate the right information during the authorization to ensure that the issuer decisioning is not driven by incorrect data.

# How to Optimize Authorization Rates

Numerous technical product solutions may be re-engineered to improve payment authorization rates. The following solutions can help merchants create win-win situations for their businesses and their customers.

## Account Updater

Some merchants store customer credit/debit card credentials to facilitate smooth recurring transactions, or to keep a card on file for a customer's future purchases. However, when payment cards expire or get lost/stolen, new card credentials are issued. Because customers generally forget to update their payment credentials at all the merchants where they have authorized a stored card, most payment card issuers (Visa®, MasterCard®, American Express®) provide account updater solutions to help merchants keep their vault fresh. These merchant systems assure smooth customer experiences, keep the merchant's authorization rates up, and reduce any unnecessary transaction processing fees.

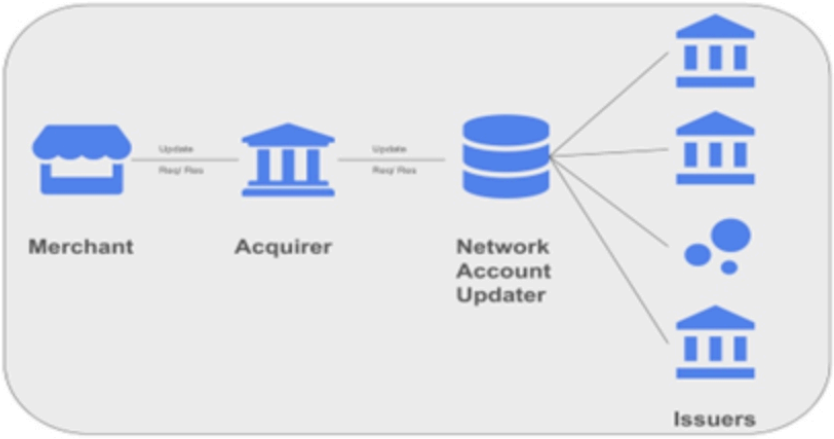


Figure 1: Payment Network Account Updater - Flow showing merchant, acquirer, network account updater, and issuer interactions

## Merchant Internal Risk-based Machine Learning/Artificial Intelligence Behavioral Models

Merchants are the first touchpoint at the start of the payment journey. Thus, when a merchant data science team develops AI/ML models centered around its customers' purchasing behavior, it arms them with the ability to extrapolate any fraudulent transactions. Critical variables that the model considers include geolocation, ticket size, merchant type, and other key data points.

Utilizing such risk-based behavioral models, merchants can derive multiple benefits:

- Lower transaction processing fee: Only transactions that are potentially less risky will be sent to the card network/issuer for approval.
- Lower chargeback rate: As risky transactions will not be authorized, the merchant will be less liable for fraudulent transactions.
- Higher authorization rate: Detecting for bad transactions early in the process ensures that merchants will attain higher authorization rates.

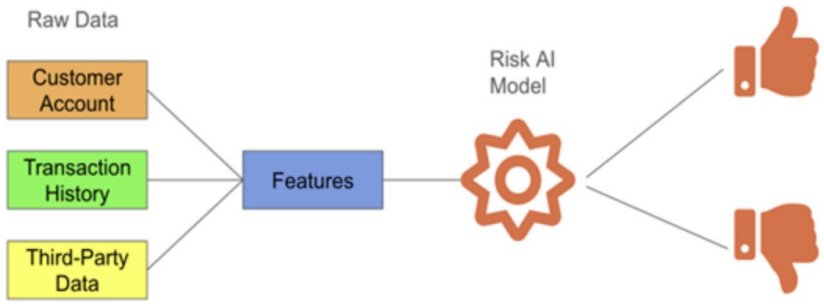


Figure 2: Risk AI Model - Feature engineering from customer account data, transaction history, and third-party data sources

## 3-DS/3-D Secure (3-Domain Structure)

This secure messaging protocol developed by EMV® enables a merchant to submit an authentication request to a card network directory server and then to the issuer/issuer access control server (ACS). This adds an extra layer of security, as issuers receive additional data elements such as IP and browser/device information in advance of the authorization. Issuers can also challenge the transaction if they see that the transaction is fraudulent, based on their risk-based authentication models.

If merchants deploy 3-DS in their transaction flow, they can reduce fraud rates and increase authorization rates, and take advantage of payment card network rules that determine the issuer's fraud liability based on whether or not the transaction was authenticated.

## Tokenization

Tokenization enables sensitive information to be stored and shared as sets of random numbers used to identify customers' payment card information. These random numbers, called tokens, can be mapped back to their payment card credentials, and can be used throughout the payment lifecycle for ecommerce transactions and specific merchants.

Tokenization enhances security by creating a unique number each time the card is used, preventing fraudsters from intruding with it, and by ensuring control mechanisms that are required for regulatory and network mandates. Because tokenization also allows for a card to be updated smoothly with new expiration dates, ensuring uninterrupted usage of the card when the physical card expires, the merchant's card vault stays fresh and leads to higher approvals. Furthermore, additional security features for issuer decisioning increases positive results. Tokens are also beneficial for customers, because if a token associated with a specific merchant is breached, there is no need to issue the physical card, since the new token for the specific merchant can be re-generated.

## ML/AI Authorization Retry Models

Artificial intelligence and machine learning models can be trained based on historical data sets, using millions of transactions with billions of data points, to understand what factors led to a payment card declination. Sometime declines are related to insufficient funds on the day of a transaction. As subscription-based merchants flourish, their need to retain customers and furnish them with world class experiences becomes crucial. AI/ML retry

models can be utilized to avoid payment failures, passive churn, and eventually lower margin loss.

Some systems work on a rule-based approach, utilizing issuer-network combinations, network regulations, and/or pre-decided thresholds, but this limits their flexibility and effectiveness. On the other hand, intensely trained ML algorithms utilizing historical purchase data and user information have proven to be very dynamic and competent in handling unknowns. Knowing the best time for charging customers and initiating retries in case of failure plays a crucial role; retry frequency rates must also be decided.

### MID and MCC Optimization

The merchant identification number (MID) is the account number provided to a merchant from an acquirer for payment processing. MCC is the merchant category code that helps identify the type of goods being sold by the merchant. Merchants that sell different types of products are assigned different MCC codes.

MCCs and MIDs are important components in issuers' authorization decisioning, as some MCC codes are riskier (i.e., gambling) to an issuer, as compared to others (i.e., utilities). Merchants open multiple MIDs and process transactions based on the MCC risk level. If less risky transactions are processed on a specific MID over time, an issuer's authorization ML/AI models will consider the MID to have a lower level of risk, based on past performance and chargebacks. This ensures the smooth processing of like transactions and increases authorization rates.

## Investing in Customer Experiences

Investing in these solutions is very important as it not only improves the customer experience, but helps in reducing fraud while managing organizational financial goals. Product, engineering, and data science teams need to come together to build an end-to-end payment authorization strategy.

To start, the product team should drive an assessment/review of the authorization rate and evaluate it against the benchmark standard in the region/country. This gives the product team an idea of where your rate stands, and what potential uplift can be attained, and thus drives the roadmap to determine which of the above solutions can be deployed. The engineering team should help in various aspects of this strategy by setting up the required infrastructure, and managing the necessary payment payloads to deliver these solutions. In this collaborative process, the data science team supports the ML/AI and experimentation aspects of these solutions.

MIDs and MCCs are the easiest strategies that can be deployed to categorize various businesses and streamline the processing on payment platforms with network and issuer. Additionally, data science teams should build an internal Risk AI/ML-based engine, as this tool is very important to help reduce the upfront risk of transactions going out of your internal payment platforms. Other strategies may be deployed based on your internal risk platform decision by performing A/B or multivariate testing. Finally, in general, tokens can provide higher approvals, and 3DS may be applied on transactions that have been identified as riskier via the internal risk AI/ML model.

---