Payment Authorization Management

The application of technology, expertise, data, and processes to improve payment authorization decision accuracy and increase the volume of legitimate transactions between merchants and customers.

FlexPay

Background

The card payments authorization ecosystem has **3 key stakeholders**:

1. Merchants who sell products and services

2. Customers who buy these products

3. Banks and other payment authorization systems. The fraud protection systems determine whether each transaction payment request is approved or declined

The payments authorization ecosystem has a simple objective: **approve all legitimate payment transactions and decline fraudulent and other undesired payment requests.** This system is enormously large and complex and requires accurate payment authorization decisions to be made in milliseconds for billions of legitimate and fraudulent payment requests.

The payments system operates in a dynamic world, supporting new sales channels and digital business models while containing growing fraud threats from bad actors and sophisticated cybercriminals.

Authorization System Facing New Challenges:

- An explosion of transactions from digital devices
- New transaction types from the gig economy
- Rapid shifts in purchase patterns from in-person purchases to eCommerce and other card-not-present purchases (accelerated by COVID-19)
- Acceleration of recurring billing services for consumers and businesses
- Massive data breaches that have given sophisticated cybercriminals deep access to stolen user identities and credit data

Core Challenges to Payments Authorization System Effectiveness

The payments authorization ecosystem has structural limitations that constrain decision accuracy, which the system is unable to correct:

Misaligned Authorization Decision Goals

The enormous losses banks incur from fraudulent transactions approved by their authorization systems ($28.6B est)* have created an incentive for banks to bias the programs in their fraud detection systems to avoid losses. The consequence of this is that the authorization algorithms routinely overcompensate decision-making for fraud avoidance. This bias towards fraud avoidance results in legitimate transaction requests that are declined based upon factors loosely associated with increased rates of fraud, rather than on the identification of direct fraud signals. These false-positive responses are called false declines.

Constraints on Authorization Decision Accuracy

Banks and 3rd party companies have built sophisticated payments authorization systems to identify and decline fraudulent transactions, but these systems work best when presented with perfect and complete information. Merchant SLAs require authorization decision results in milliseconds. This short time to make decisions, when combined with limits on information access during the approval process, place significant constraints on decision accuracy.

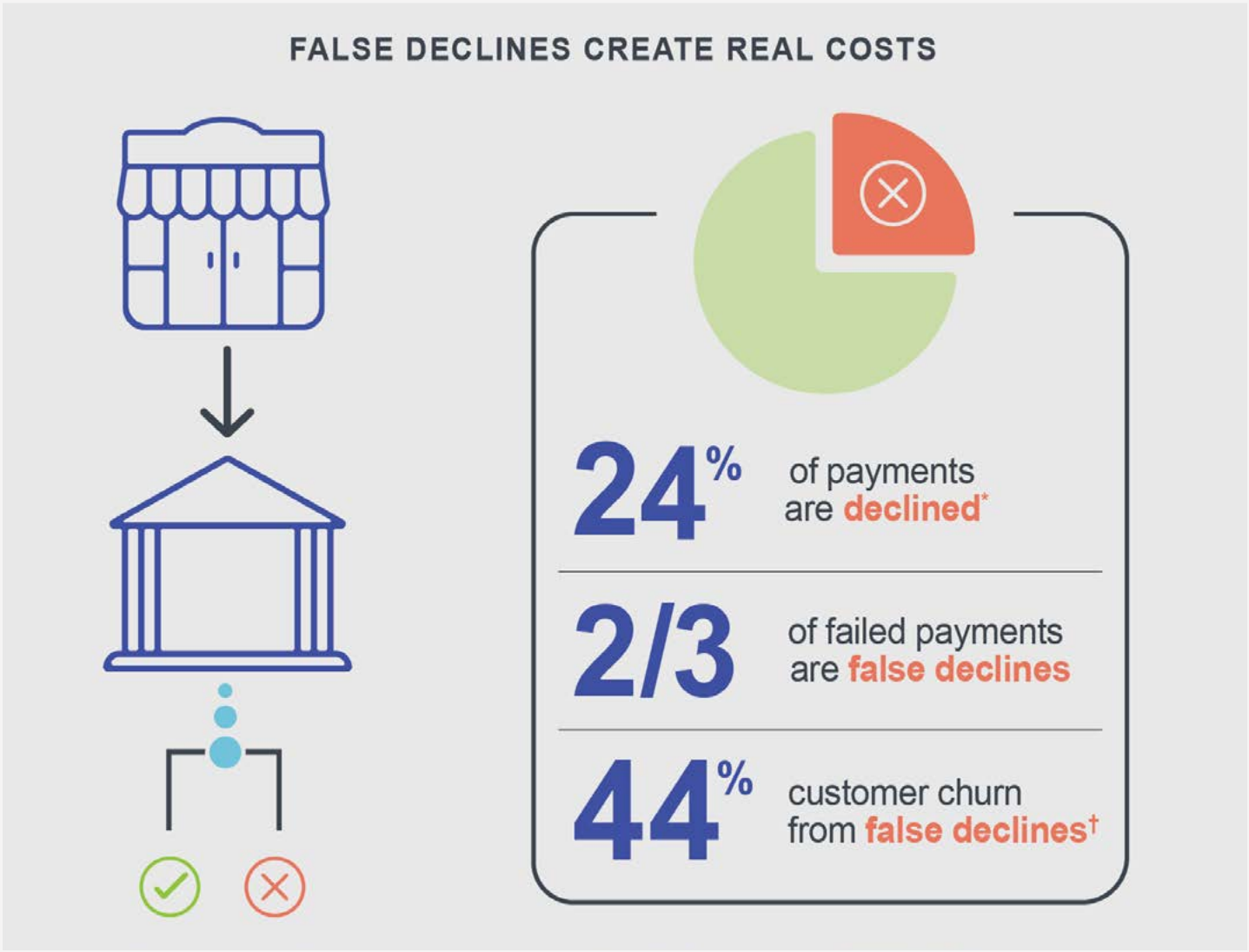
These and other factors have led to these costly errors in today's payments authorization system:

1. Approval decisions on a percentage of truly fraudulent transactions - causing pain in the form of fraud losses for banks and chargebacks for merchants

2. Decline decisions on legitimate transactions - causing pain for merchants and customers

The cost of fraud losses to banks and merchants is well documented due to financial reporting requirements and chargeback reporting. However, the cost of declines on legitimate transactions, or false declines, is less understood because this burden has been shifted to and distributed across the millions of merchants and customers who use the system.

* Aite Group Report



In addition to fraud authorization declines, payment requests can also be declined for other reasons, including insufficient funds (NSF), data issues, system incompatibilities, and payment gateway errors.

Failed payments and false declines create a devastating problem for merchants, imposing opportunity costs orders of magnitude larger than the direct losses to banks and merchants caused by fraud.

According to the Aite Group, global false declines alone will cost merchants over $443B in lost revenue from payment decline decisions in 2021.

The $443B in lost merchant revenue is more than the GDP of 182 countries

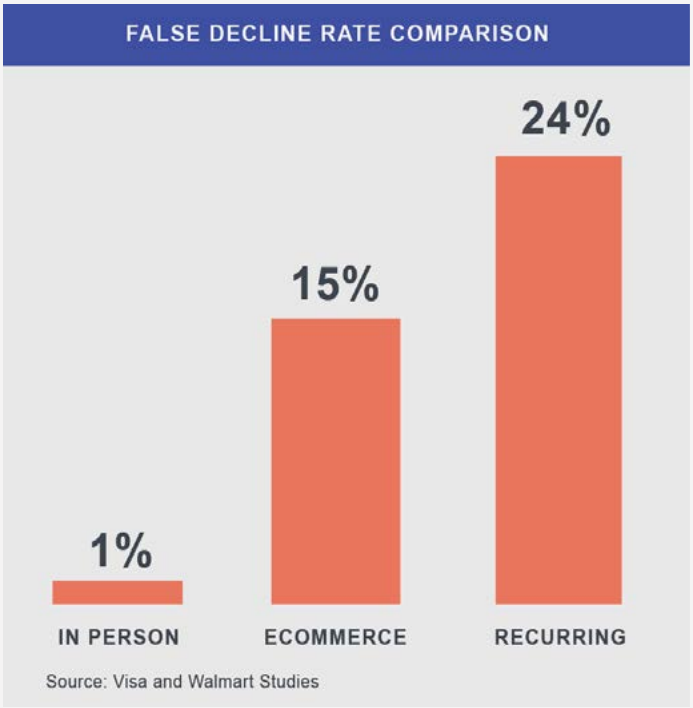
* Visa and Walmart Studies
† Javelin Report

Authorization Decision Errors – A Deeper Dive

False declines are not distributed evenly across all merchants or transaction types.

Studies by Visa and Walmart have shown that the payment authorization systems use stricter criteria on payment decisions from purchases where the merchant does not scan the card (Card-Not-Present, or CNP transactions) due to the higher incidence of fraud on eCommerce and other CNP transaction types.

Not surprisingly, CNP transactions generate a much higher frequency of failed payments. This chart shows relatively low false decline rates for in-person transactions, compared to the much higher rate of false declines occurring on recurring or subscription renewal payments.



False declines are particularly harmful for subscription products and services that use recurring billing models, causing additional harm beyond the failed payment itself. In fact, FlexPay research shows that payment failures cause up to 48% of all customer churn for subscription businesses. When a false decline occurs on a subscription service, service or product delivery is paused, negatively impacting both the merchant and the customer.

- The merchant is harmed because profitable customer acquisition investments require a minimum number of successful billing cycles and lifetime value, or LTV, before profitability is reached. The interruption in each customer's billing caused by failed payments stops ongoing revenue, reducing profitability. Reductions in customer LTV limit the customer acquisition cost (CAC) that companies can invest to acquire more customers.

- The customer is harmed because the convenience they seek from the regular service delivery provided by a subscription model is broken.

Payment Authorization Management

Payment Authorization Management (PAM) is the category name for FinTech solutions that help improve the accuracy of payment authorization decisions.

PAM helps reduce fraudulent transactions, approve more legitimate transaction settlements, and recovers more revenue from failed payments.

Payment Authorization Management applications are 3rd party technology solutions that site outside the payment ecosystem, operating as a middle layer between merchants, customers, and payment authorizers. These solutions help improve the performance of the payments system, supplementing the accuracy of payment authorization decisions and reducing decision errors. By helping complete more legitimate payment transactions, PAM reduces the hundreds of billions of dollars currently lost in declines, closing the gap to the goal of 100% completion of legitimate transactions.

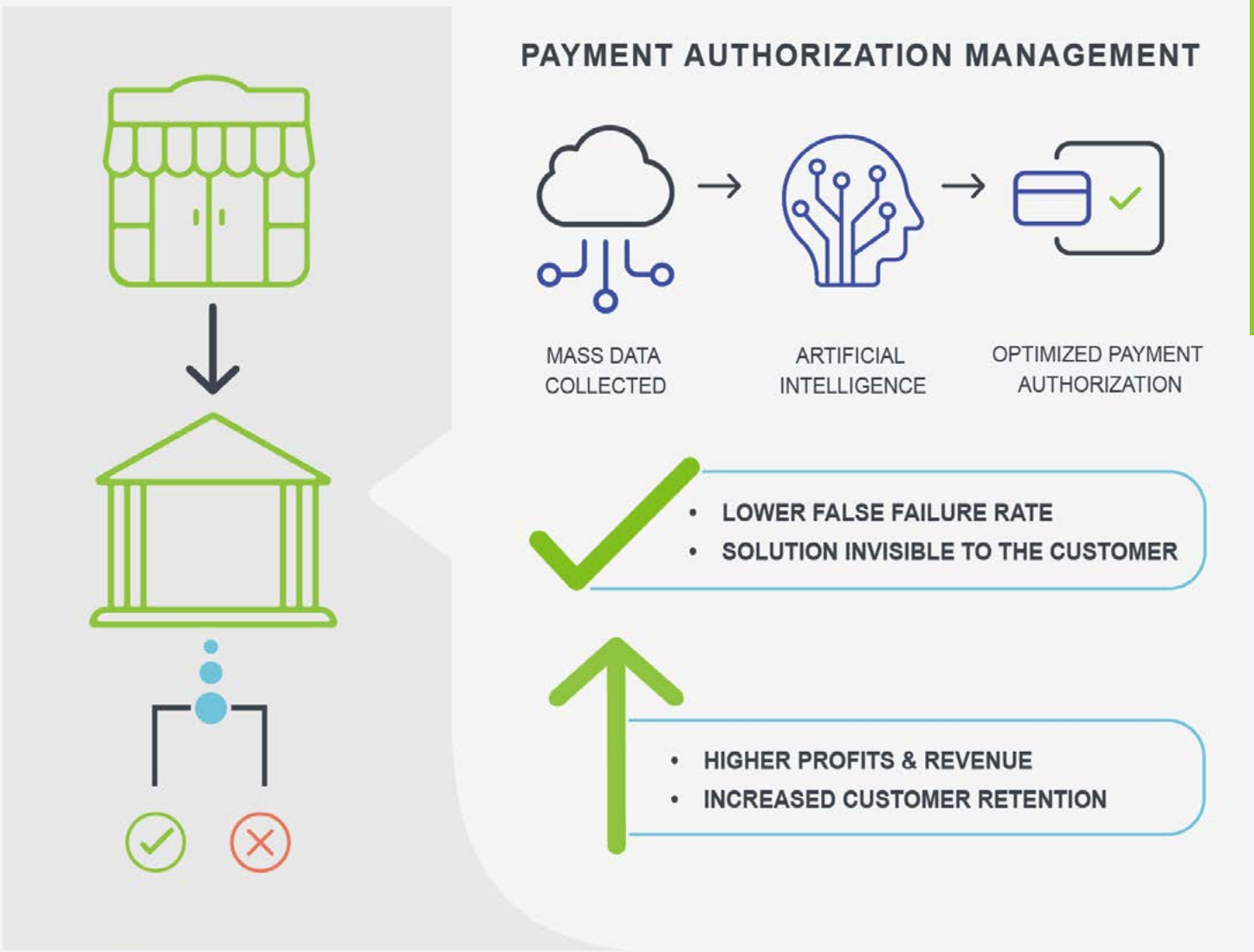
PAM benefits the ecosystem and its participants, fixing systemic limitations in the system. PAM solutions operating outside the ecosystem apply data, technology and processes to improve decision accuracy.

The sophistication of cybercriminals and the complexity of fraud prevention algorithms lead to payment decision errors that are triggered for a wide variety of reasons. AI (artificial intelligence) and ML (machine learning) are tools uniquely suited for PAM solutions to solve authorization decision errors, compared to rules-based solutions that follow one script for every transaction recovery attempt.

Authorization decision errors are caused by a wide range of reasons. This complexity requires high-performance PAM solutions to deploy strategies individualized for each individual transaction and be able to adapt when decision errors occur.

PAM best practices:

- AI/Machine Learning technology capable of autonomously creating individualized payment submission strategies, optimized for authorization accuracy
- Algorithms trained on giga datasets (billions) of authorization records containing both accurate and inaccurate decisions
- Algorithms coded with payments ecosystem knowledge to deliver dramatically improved authorization results
- Cloud-based solution supported by broad API capabilities for easy integrations with payment gateway and CRM/billing systems, providing the scale and interoperability required for major networks
- Solutions invisible to the end-customer, thereby eliminating the need to introduce poor customer experiences, and the need for customers to seek help solving payment problems they didn't create



Some companies have recognized the tremendous cost to merchants and customers and have created simplistic solutions to address authorization decision errors, particularly for false decline transactions. It is evident that rules-based approaches or manual dunning solutions do not deliver the performance levels of true PAM solutions and should be considered inferior alternatives to PAM solutions.

Deploying a PAM strategy is one of the easiest and most effective programs a company with subscription or recurring billing can implement to increase customer retention and decrease churn.

Summary

Merchants and customers depend on an **efficient payment ecosystem** to support easy purchase settlements for all legitimate transactions.

- It is critical for merchants to adopt a Payment Authorization Management (PAM) strategy for their businesses.
- Reducing or removing the friction that prevents completion of all consenting and legitimate transactions with customers is mission-critical to realizing full growth and profit potential.
- Any issues with the accuracy of the payment authorization system impart an enormous cost to merchants because of the high percentage of purchases made through the system. The merchant cost is accelerated for eCommerce businesses and is even higher for subscription businesses and recurring billing models that sell goods and services.
- New technologies and solutions are required to solve this problem. It has been proven that manual processes or simplistic rules/process-based attempts to correct authorization errors fall significantly short of AI and advanced ML-powered solutions' potential.
- PAM solutions deliver payment settlement success that is invisible to the end-customer, which is superior to approaches requiring end-customer involvement because customer exposure to false declines contributes to customer churn.

CONNECT WITH FLEXPAY

1-800-273-4689 | info@flexpay.io | Linkedin/flexpay