Visa Consulting & Analytics (VCA)

Helping to maximize merchant success through authorization and fraud prevention

In today's evolving payments ecosystem, merchants face an ongoing challenge: they need to boost authorization rates and increase revenues while also protecting themselves from rapidly evolving fraud trends. As digital commerce grows, so does the sophistication of fraudulent activities. Merchants who prioritize robust authorization strategies and invest in fraud-prevention tools are better positioned to protect their brand, reduce revenue loss, and enhance customer satisfaction.

Newest in Visa Consulting & Analytics' insights series, What's influencing payments in 2025: 10 recommendations on business strategy, Visa consultants deep-dive into the rapidly evolving fraud landscape, highlight recent trends, and outline fraud-prevention strategies for today's merchants.

In the last two years, card-present (CP) fraud rates have decreased by about

85%

while card-not-present (CNP) fraud continues to rise as ecommerce grows.[1]

Fueled by increased access to technology and facilitated by the illicit networks and tools available on the dark web, financial cybercrime has advanced from basic card theft to more complex attacks: account takeovers, the creation of synthetic identities, and large-scale data breaches.

A single high-profile breach or spike in fraudulent transactions can damage a merchant's brand. Consumers are unlikely to return to businesses they perceive as not secure. Fraud also results in financial losses due to chargebacks, where customers dispute and reverse transactions, as well as through reimbursements and loss of goods or services. On the other hand, friction caused by false declines or complicated authentication processes can lead to consumer frustration and cart abandonment.

Fraud trends are dynamic. VisaNet data shows some forms of fraud, such as counterfeit card fraud, have declined due to the adoption of chip technology. In the last two years, card-present (CP) fraud rates have decreased by about 85 percent, while card-not-present (CNP) fraud continues to rise as ecommerce grows.[1] Fraudsters are using automated bots and ever-advancing phishing schemes to steal cardholder credentials, making it vital for merchants to stay ahead with adaptive, effective fraud-prevention tools.

Enhancing card-authorization rates is essential for merchants looking to improve customer experience and satisfaction, build a trustworthy brand, and help maximize business performance in a highly competitive market. Since many card transactions involve small, everyday purchases, monitoring approval rates can offer valuable insights into customer behavior and overall satisfaction. Other than in CEMEA, all regions have seen year over year decreases in overall approval rates. Notably, the U.S. reports the lowest approval rates, which have fallen below 87 percent.[1]

Enhancing card-authorization rates is essential for merchants looking to improve customer experience and satisfaction, build a trustworthy brand, and help maximize business performance in a highly competitive market.

Techniques to optimize authorization rates

A key aspect of increasing merchant success is helping legitimate transactions are approved and false declines are decreased.

The role of tokenization

Tokens replace sensitive card data with unique, transaction-specific identifiers, which streamline the payments process and enhance security throughout the transaction lifecycle. When tokens are used, sensitive card information is replaced and reduces the risk if the data were to be intercepted via data breach or leak. By helping minimize exposure to fraud, tokenization can assist in reducing declines due to suspected fraud, which is the second highest decline reason globally, and increases issuer confidence in approving transactions.The average global token adoption from Q1 2024 to Q1 2025 increased by 6%.[1]

T

The average global token adoption from Q1 2024 to Q1 2025 increased by

6%[1]

Involving the issuer in authentication

To help verify cardholders during CNP transactions, some merchants use 3D Secure (3DS), a solution designed to help reduce unauthorized transactions by adding a second authentication step and by involving the issuer in the transaction flow. For merchants, 3DS provides a liability shift for fraud-coded chargebacks where the issuer is responsible for the unauthorized charge and not the merchant.

Alternatives to 3DS include real-time data sharing solutions that send enhanced information to issuers before authorization, which is particularly valuable for CNP transactions. The exchanged data between the merchant and issuer about their shared customer can assist in helping reduce false declines.

Establishing an active decline mitigation strategy

Unnecessary declines can impact a merchant's bottom line and customer relationships. Some attempted transactions with certain decline codes (known as soft declines) can be retried to complete a successful payment. For example, transactions declined due to a cardholder's insufficient funds, which is the most common reason for card decline across all regions, can be reattempted after a reasonable waiting period to allow the customer to address the issue. However, a lost or stolen card decline message, referred to as a hard decline, should not be reattempted.

For merchant-initiated transactions, such as recurring transactions, merchants can help ensure stored card details are current by notifying customers ahead of upcoming subscription charges. This helps minimize surprises and reduces the likelihood of declines, thus increasing payment success and improving customer satisfaction.

Best practices for fraud detection and prevention

To help navigate the complexities and challenges of today's online fraud environment while simultaneously balancing risk mitigation with enhanced customer experience, Visa consultants recommend the following six practices to merchants:

Deploy pre-authorization fraud checks

Deploying real-time screening tools that analyze transactions before they are sent to the issuer for authorization can help prevent fraudulent attempts from impacting approval rates.

Utilize machine learning (ML) and artificial intelligence (AI)

Device fingerprinting and biometrics use advanced algorithms to detect suspicious patterns and adapt to new fraud tactics. Machine learning can identify anomalies in transaction behavior that may bypass traditional rule-based fraud detection systems.

Decrease operational time spent on fraud screening

Automation can assist with blocking transactions that match known fraud patterns, which frees up staff time for more complex investigations.

Conduct frequent reviews and re-evaluations

A fraud strategy requires continuous monitoring and re-evaluation to help ensure it is effective against emerging threats. It is important to regularly adjust fraud detection parameters and review recent fraud cases for new patterns.

Use smart velocity checks

Set velocity thresholds around transaction frequency within a specific timeframe.

Analyze geolocations and IP addresses

Cross-reference customer location data and monitor for mismatches between shipping and IP geolocations.

How Visa can help

In a payments landscape marked by constant change, merchants must proactively invest in both fraud prevention and authorization optimization. Data-driven tools, machine learning, and advanced authentication mechanisms not only protect against losses, but can also help merchants build customer loyalty and drive business growth. By working with VCA and adopting best practices, merchants can help maximize their success, reduce risk, and provide frictionless payments experiences to foster long-term customer relationships.

Visa solutions for merchants

The VCA team can work with merchants to identify areas of opportunity to optimize their approach to authorization and fraud prevention. Visa has the following solutions to assist in mitigating fraud and increasing acceptance.

Visa Protect Risk Insights

A data-driven platform that provides merchants and financial institutions with real-time analytics and actionable intelligence to identify, monitor, and mitigate payments fraud and risk

Visa Token Services

Facilitates tokenization for higher approval rates and greater security, ushering in a more secure era of e-commerce

Visa Data Only

Enables enhanced data sharing between merchants and issuers for better decision-making

Visa Account Updater

Securely provides merchants and payment processors with updated cardholder information (e.g., new account numbers or expiration dates) to help avoid any interruption in recurring payments and to reduce transaction declines

Featurespace

Integrates advanced AI into its fraud prevention and risk-scoring offerings. This enhancement provides real-time detection of sophisticated fraud attacks, ensuring businesses stay safe without adding friction to the user experience

Partial Authorization

Ability to approve a transaction for a portion of the requested amount when a cardholder's available balance is insufficient, allowing the customer to use another form of payment for the remaining balance

Based on Global VisaNet data from the last eight quarters (unless otherwise noted), the following exhibits highlight the top three reasons for declined transactions by amount globally. Understanding these key drivers can help identify opportunities to improve approval rates and enhance customer experience:

Top three decline reasons (Globally) by amount*

#1	#2	#3
Not Sufficient Funds	Suspected Fraud	Exceeds Approval Amount

*Ranking is unchanged by individual region

About Visa Consulting & Analytics

We are a global team of thousands of payments consultants, data scientists and economists across six continents.

- ✓ Our consultants are experts in strategy, product, portfolio management, risk, digital and more with decades of experience in the payments industry.
- ✓ Our data scientists are experts in statistics, advanced analytics and machine learning with exclusive access to insights from VisaNet, one of the largest payment networks in the world.
- ✓ Our economists understand economic conditions impacting consumer spending and provide unique and timely insights into global spending trends.

The combination of our deep payments consulting expertise, our economic intelligence and our breadth of data allows us to identify actionable insights and recommendations that drive better business decisions

To get started, reach out to your Account Executive directly. Learn more about the team, resources, and our data-backed insights on Visa.com/VCA, and follow the team on LinkedIn.

[1] Global VisaNet data from April 2023 - March 2025 for all regions (EU, AP, LAC, CEMEA, US and Canada)

Forward-looking statements. This content may contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. Forward-looking statements generally are identified by words such as "believes," "estimates," "expects," "intends," "may," "projects," "could," "should," "will," "continue" and other similar expressions. All statements other than statements of historical fact could be forward-looking statements, which speak only as of the date they are made, are not guarantees of future performance and are subject to certain risks, uncertainties and other factors, many of which are beyond our control and are difficult to predict.

Third-party logos. All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa.

As-Is Disclaimer. Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.